Act No. 412/2005 Coll.

ACT
of 21st September 2005

on the Protection of Classified Information and Security Eligibility

Amendment: Act No. 119/2007 Coll.
Amendment: Act No. 177/2007 Coll.
Amendment: Act No. 296/2007 Coll.
Amendment: Act No. 32/2008 Coll.
Amendment: Act No.124/2008 Coll., Act No. 126/2008 Coll.
Amendment: Act No.250/2008 Coll.
Amendment: Act No. 41/2009 Coll.
Amendment: Act No. 227/2009 Coll.
Amendment: Act No. 281/2009 Coll.
Amendment: Act No. 255/2011 Coll., Act No. 420/2011 Coll.
Amendment: Act No. 167/2012 Coll.
Amendment: Act No. 458/2011 Coll.

The Parliament of the Czech Republic has resolved upon the following Act:

PART ONE
GENERAL PROVISIONS

Section 1

Subject of the Act

This Act regulates the principles for determination of information as classified information, conditions for access to it and further requirements for its protection, principles for determination of sensitive activities and conditions for their perfomance and related performance of the state administration.

Section 2

Definition of terms and concepts

For the purpose of this Act

a) classified information shall be any information recorded on any medium, regardless of its form, designated as such in accordance with this Act, whose unauthorized divulgence, disclosure, misappropriation or misuse could cause damage to the interest of the Czech Republic or could be unfavourable to this interest and that is specified on the list of classified information (S. 139);

b) interests of the Czech Republic shall be preservation of its constitutionality, sovereignty and territorial integrity, securing of internal order and security, international obligations and defence, protection of economy and protection of the life or health of natural persons;

c) the breach of the duty to protect classified information shall be the breach of any obligation imposed by this Act or stipulated on the basis of this Act;

d) the State body shall be an organizational body of the state in accordance with a special legal regulation, region, Prague, the capital city and its metropolitan districts and communities which exercise the state administration in cases determined by special legal regulations; as State bodies are considered to be also the Security Information Service, the Military Intelligence and the Czech National Bank;

e) the responsible persons shall be

1. minister in case of a Ministry;
2. competent head in case of other central administrative body;
3. responsible person in the organizational State body carrying out the function of promoter in case of an organizational State body established by another organizational State body;
4. competent head in case of other organizational state bodies;
5. directors in case of Security Information Service and Military Intelligence;
6. governor in case of Czech National Bank;
7. director in case of a regional autority;
8. director of the Metropolitan authority of the Capital City Prague;
9. secretary of the metropolitan district authority of the capital city Prague, if there in no such secretary, the metropolitan district mayor;
10. secretary of the Metropolitan authority in case of statutory town;
11. secretary of the town/community authority in case of other towns and communities, if there is no such secretary, the /town community mayor;
12. responsible person of the territorial self-governing unit carrying out the function of promoter in case of the structural component of the territorial self-governing unit;
13. authorized representatives in case of legal entities not mentioned in points 6 -11; should more persons act in the name of these other legal entities according to the special legal regulation as authorized representatives, or should a person who is not the authorized representative act accordingly, then the person authorized to act in subject-matters regulated by this Act shall be the only responsible person; and
14. natural person pursuing business;

f) originator of the classified information shall be a State body, legal entity or natural person pursuing business that released the classified information, or the Office of Industrial Property according to S. 70 par. 4;

g) foreign power shall be a foreign state or its authority or multinational or international organisation or their autority;

h) unauthorized person shall be a natural person or legal entity that does not meet conditions to access classified information as stated in this Act;

i) briefing shall be a written record that the natural person concerned has been briefed on his/her rights and obligations in the area of protection of classified information and on the consequences of their violation;

j) security standard shall be a classified set of rules defining procedures, technological solutions, security parameters and organizational measures to secure the lowest possible level of protection of classified information;
k) security operational mode shall be an environment, in which the information system operates, characterized by the security level of classified information being processed and by the security clearance levels of users.

PART TWO

PROTECTION OF CLASSIFIED INFORMATION

CHAPTER I

Introductory provisions

Section 3

Detriment to the interest of the Czech Republic and disadvantageousness to the interest of the Czech Republic

1.

(1) For the purpose of this Act detriment to the interest of the Czech Republic shall be damage to or endagering of the interest of the Czech Republic. Depending on the seriousness of the damage caused or of the seriousness of the threat to the interest of the Czech Republic, the detriment shall be structured as extremely serious detriment, serious detriment or simple detriment.

(2) Extremely serious detriment to the interest of the Czech Republic arises in the case of disclosure of classified information to unauthorized person or in the case of misuse of classified information, which can result in

a) immediate endangering of sovereignty, territorial integrity or democratic principles of the Czech Republic;
b) vast losses of human lives or vast threat to life and limb of citizens;
c) extremely serious or long-term damage to the economy of the Czech Republic;
d) significant breach of internal order and security of the Czech Republic;
e) extremely serious endangerment of important security operations or activities of intelligence services;
f) extremely serious endangerment of activities of the North Atlantic Treaty Organisation, European Union or any member state;
g) extremely serious endangerment of the combat capability of the Armed Forces of the Czech Republic, of the North Atlantic Treaty Organisation or its member state or of the member state of the European Union, or
h) extremely serious damage to diplomatic or other relations of the Czech Republic towards the North Atlantic Treaty Organisation, European Union or member state.

(3) Serious detriment to the interest of the Czech Republic arises in the cases of disclosure of classified information to any unauthorized person or in the case of misuse of classified information, which can result in

a) endangering sovereignty, territorial integrity or democratic principles of the Czech Republic;
b) significant damage to the Czech Republic in the financial, monetary or economic areas;
c) losses of human lives or threat to life and limb of citizens;
d) breach of internal order and security of the Czech Republic;
e) serious endangerment of the combat capability of the Armed Forces of the Czech Republic, of the North Atlantic Treaty Organisation or its member state or of the member state of the European Union;
f) serious endangerment of important security operations or activities of intelligence services;
g) serious endangerment of activities of the North Atlantic Treaty Organisation, European Union or any member state;
h) serious damage to diplomatic or other relations of the Czech Republic towards the North Atlantic Treaty Organisation, European Union or any member state or other state; or
i) serious escalation of international tension.

(4) Simple detriment to the interest of the Czech Republic arises as a consequence of disclosure of classified information to any unauthorized person or misuse of classified information, which can result in

a) worsening of relations between the Czech Republic and a foreign power;
b) endangering of the individual´s security;
c) endangering of the combat capability of the Armed Forces of the Czech Republic, the North Atlantic Treaty Organisation or its member state or of a member state of the European Union;
d) endangering of security operations or activities of intelligence services;
e) endangering of activities of the North Atlantic Treaty Organisation, of the European Union or any of its member states;
f) obstructing, impeding or endangering of the vetting procedure or investigation of especially serious offences or facilitation of their commission;
g) occurrence of damage not insignificant to the Czech Republic;
h) serious infringement of the economic interests of the Czech Republic.

(5) Disadvantageous to the interests of the Czech Republic is the disclosure of classified information to any unauthorized person or misuse of classified information, which can result in

a) breach of activities of the Armed Forces of the Czech Republic, the North Atlantic Treaty Organisation or its member state or of the member state of the European Union;
b) obstructing, impeding or endangering of the vetting procedure or investigation of offences other than stated in the paragraph 4 f) or facilitation of their commission;
c) damage to important economic interests of the Czech Republic or to economic interests of the European Union or its member states;
d) breach of important commercial or political negotiations between the Czech Republic and a foreign power; or

e) breach of security or intelligence operations.

Section 4

Security classification levels

Classified information shall be categorised according to the security classification levels into

a) TOP SECRET if its unauthorized disclosure or its misuse can result in extremely serious detriment to the interests of the Czech Republic;
b) SECRET if its unauthorized disclosure or its misuse can result in serious detriment to the interests of the Czech Republic;
c) CONFIDENTIAL if its unauthorized disclosure or its misuse can result in simple detriment to the interests of the Czech Republic;
d) RESTRICTED if its unauthorized disclosure or its misuse can be disadvantageous to the interests of the Czech Republic.

Section 5

Types of securing the protection of classified information

Protection of classified information shall be ensured by

a) personnel security, which consists of selection of natural persons who should have access to classified information, verification of conditions for their access to classified information, their training and protection;
b) industrial security, which consists of a system of measures to ensure and verify conditions for access of a facility to classified information and to secure handling of classified information on the part of a facility in accordance with this Act;
c) administrative security, which consists of a system of measures to provide originating, receiving, recording, handling, sending, transportation, transmission, hand carriage, storing, discarding, archiving, or other types handling of classified information;
d) physical security, which consists of a system of measures designed to prevent or impede unauthorized access, or to provide evidence of any access or of any attempted access;
e) security of information and communication systems, which consist of a system of measures to provide confidentiality, integrity and availability of classified information handled by these systems, and liability of the administration and user for their implementation in information or communication systems; and
f) cryptographic protection, which consists of a system of measures for the protection of classified information using cryptographic methods and cryptographic materials in processing, transmission or storing of classified information.

CHAPTER II

Personnel security

Conditions for access of natural persons to classified information at the level RESTRICTED

Section 6

(1) Natural person may be granted access to RESTRICTED classified information in case he/she needs it in order to perform his/her official tasks or activities (on a need-to-know basis), further, who is a holder of the Notice of compliance allowing the access to RESTRICTED classified information (hereinafter referred to as „the Notice"), of the Personnel Security Clearance (hereinafter referred to „the PSC") (S. 54) or of the Certificate (S. 80) and has been security briefed, save as otherwise provided for in this Act or in the special legal regulation (S. 58-62).

(2) The Notice will be issued to the natural person who

a) has full legal capacity;
b) is aged 18 or over
c) has no criminal record.

(3) Fulfilment of the conditions stated in paragraph 2 shall be verified and the Notice to the natural person shall be issued by the person who is responsible towards this natural person in a official service relationship or labour-law relationship, member relationship or similar relationship or by a person authorized by this responsible person. If there is no such responsible person according to the first sentence, the compliance with conditions outlined in paragraph 2 shall be verified and the Notice to the natural person shall be issued by a responsible person or by a person authorized by the responsible person who allows access to classified information to the natural person at the classifiaction level RESTRICTED. In other cases, fulfilment of the conditions stated in paragraph 2 shall be verified and the Notice shall by issued by the National Security Authority (hereinafter referred to as „ the Authority") on the basis of a reasonable written request.

Section 7

(1) The condition of legal capacity shall be proved by the natural person´s statement of legal capacity. The condition of age shall be proved by the natural person´s identification card or by travel documents. The condition of no criminal record shall be proved by a statement of criminal records and, in the case of a foreigner, by a similar document issued by the person's country of citizenship, as well as by the document of the country in which the person has resided for at least 6 consecutive months. The documents certifying no criminal records shall apply only for 3 months from the date of their issuance.

(2) Documents stated in paragraph 1 shall be submitted by the natural person.

(3) The form of the statement of the legal capacity of the natural person shall be

determined by the implementing legal regulation.

Section 8

Clean record

12. The condition of clean record is met by the natural person who has not been condemned upon final and conclusive judgement of an intentional crime or of a crime related to the protection of classified information, or by the natural person who is regarded as not to be condemned.

13.

14.

Section 9

(1) Prior to initial access to classified information at the security classification level RESTRICTED the briefing of the natural person shall be arranged by the person who is responsible towards this natural person in a framework of the official service relationship or labour-law relationship, member relationship or similar relationship. If there is no such responsible person according to the first sentence, the briefing shall be arranged by the responsible person of the authority that will grant access to classified information. The aknowledgement shall be signed by the natural person concerned and by the individual who conducted the briefing; one copy will be forwarded to the briefed person and one copy will be stored.

15.

(2) The issuing authority of the Notice shall verify every 5 years from the date of its issuance fulfilment of conditions laid down in S. 6 par. 2a) and c); fulfilment of these conditions may be verified by the authority even before the expiration of the stated period in case of reasonable doubts indicating that the person concerned no longer fulfils any of these conditions.

16.

(3) Validity of the Notice expires or will be terminated

17.

a) upon delivery of a written notification of the issuing authority of the Notice stating that the natural person no longer fulfils condition outlined in S. 6 par. 2a) or c);
b) by termination of the official service relationship or labour-law relationship, member relationship or similar relationship within the framework of which the natural person had access to classified information;
c) by commencement of the official service relationship or labour-law relationship, member relationship or similar relationship within the framework of which the natural should have access to classified information if the Notice has been issued by the responsible person or by a person authorized by the responsible person of the body making access of the natural person to classified information possible, or by the Authority in accordance with S. 6 par. 3;
d) upon death or upon declaration of death of the person concerned;
e) as a result of theft or loss;
f) as a result of damage that causes illegibility or destroys its integrity;
g) upon delivery of a written notification of the issuing authority of the Notice stating that the natural person did not fulfil conditions stated in S. 10 par. 2b) within the prescribed period;
h) by return of the Notice to the issuing body or, if there is no such body, to the Authority;

i) on the fifteenth day after delivery of the Personnel Security Clearance (the PSC) or of the Certificate, or

j) upon change of any data included therein.

(4) When the validity of the Notice terminates according to par. 3a) and g), the issuing authority of the Notice shall prevent the natural person concerned from having access to classified information and shall notify in writing the natural person thereof. The reasons of termination of the validity of the Notice shall be given in this written notification. If the validity of the Notice was terminated according to par 3 b) to d), f), h) or i) the issuing authority of the Notice shall make the written record thereof and store it.

18.

(5) Access of the natural person to classified information is not affected by termination of the validity of the original Notice according to par. 3 e), f) or j) if the holder of the Notice asks in writing the issuing autority within 15 days after termination of its validity to issue a new Notice; in this case the issuing authority of the Notice shall grant a new Notice within 5 days after delivery of the written request, which substitutes the original Notice.

(6) When the validity of the Notice terminates according to par. 3 a) or g), the natural person shall forward the Notice within 15 days after the delivery of the written notification thereof, and in case of termination according to par. 3 b), c) or i), within 15 days after this termination to the issuing authority of the Notice.

(7) In case of termination of the validity of the Notice it shall be assumed that the natural person has not been briefed.

(8) The forms of Notice and briefing shall be set by the implementing legal regulation.

19.

20.

21. **Section 10**

22.

(1) Conditions outlined in S. 6 par. 2 a) and c) must be fulfilled by the natural person, who is the holder of the Notice, throughout the whole period of access to classified information at the security classification level RESTRICTED.

23.

(2) The natural person stated in paragraph 1 shall

24.

a) notify in writing the issuing authority of the Notice of

1. a change concerning conditions outlined in S. 6 par. 2a) and c);
2. theft, loss or damage of the Notice;
3. date of delivery of the PSC or the Certificate;
4. facts outlined in S. 9 par. 3 c), f) and j);

within 15 days of the date when this change or fact occurred or upon learning of the change by the natural person.

b) submit within a prescribed period, in cases according to S. 9 par. 2, at the request of the issuing authority of the Notice, a statement of criminal records, in case of foreigner similar document issued by his/her state of origin as well as by the state, where the foreigner resided at least for 6 consecutive months in the last 5

years, and a statement of the natural person of the legal capacity; these documents shall not be older than 3 months.

Conditions for access of a natural person to classified information at security classification levels TOP SECRET, SECRET or CONFIDENTIAL

Section 11

(1) Only such natural person may be granted access to TOP SECRET, SECRET or CONFIDENTIAL classified information, whose duties, work, or other functions necessarily require such access, who is a holder of a valid PSC (S. 54) at the appropriate security classification level and who has been briefed, save as otherwise provided for in this Act or in the special legal regulation (S. 58 - 62).

(2) Prior to the initial access to classified information at security classification levels TOP SECRET, SECRET, CONFIDENTIAL, the briefing of the natural person shall be arranged by the person who is responsible in respect of this natural person in a framework of the service relationship or labour-law relationship, member relationship or similar relationship. In case of no such responsible person according to the first sentence, the briefing shall be arranged by the responsible person of the authority that may grant access to classified information. The briefing shall be acknowledged by the natural person concerned and by an individual who conducted the briefing; one copy will be forwarded to the briefed person, one copy will be stored and one copy will be sent to the Authority. The obligation to send one copy of the briefing does not apply to the Intelligence Services of the Czech Republic (hereinafter referred to as "Intelligence Services") in the cases stated in S. 140 par. 1 a), and to the Ministry of the Interior in the cases stated in S. 141 par. 1.
25.

(3) The briefing of the Director of the Authority and of the Director of the Intelligence Services will be carried out by the Prime Minister, the briefing of the Director of the Office for Foreign Relations and Information will be carried out by the Minister of the Interior and the briefing of the Director of the Military Intelligence will be carried out by the Minister of Defence; paragraph 2 shall apply similarly concerning acknowledgement, sending and storing of the copy of the acknowledgement.

(4) In cases of termination of the validity of the PSC (S. 56 par. 1) or termination of service relationship or labour-law relationship, membership relationship or similar relationship, in the framework of which the natural person has been granted access to classified information, it is assumed that the natural person has not been briefed.

Section 12

Conditions for issuance of the Personnel Security Clearance (the PSC)

(1) The Personnel Security Clearance (the PSC) will be issued by the Authority to the natural person, who

a) is a citizen of the Czech Republic or a citizen of any member state of the European Union or of the North Atlantic Treaty Organization;

b) meets the conditions outlined in S. 6 par. 2;
c) is personally eligible;
d) is security reliable.

(2) Conditions outlined in paragraph 1 shall be met by the natural person throughout the whole period of the validity of the PSC (S. 55).

Section 13

Personal eligibility

(1) The condition of personal eligibility will be fulfilled by the natural person who does not suffer from any disorder or problem that could affect his/her reliability or ability to maintain confidentiality of information.

(2) Personal eligibility according to paragraph 1 will be verified on the basis of the statement of personal eligibility and in the cases determined by this Act (S. 106) also on the basis of expert reports on the personal eligibility.

(3) The Intelligence Service will verify the personal eligibility of its members, employees and job or service candidates in cases stated in S. 140 par. 1 a), and the Ministry of Interior in cases stated in S. 141 par. 1, on the basis of a statement concerning personal eligibility or on the basis of psychological examination by psychological centre of the Intelligence Service or of the Ministry of Interior.

Section 14

Security reliability

(1) The condition of personal reliability will be fulfilled by the natural person in case of whom no security risk has been ascertained.

(2) The following shall be considered to be a security risk

a) serious or repeated activities against the interests of the Czech Republic;
b) activities consisting of suppressing of human rights or liberties, or support of such activities;
c) fact of unexplained property affluance with respect to duly declared income of the natural person.

(3) Also the following may be considered to be a security risk

a) assignment to the intelligence or counterintelligence unit of the former State Security, to the Intelligence Department of the General Staff of the Czechoslovak People's Army or to the Internal Protection Department of the Correctional Treatment Facility, or provable co-operation with the former State Security or with the Intelligence Department of the General Staff of the

Czechoslovak People's Army or with the Internal Protection Department of the Correctional Treatment Facility;

b) use of another identity;

c) intentional breach of legal regulations that can result in damage to interests of the Czech Republic;

d) conduct that may render the individual liable to influence and may affect his or her trustworthiness or ability to maintain confidentiality of information;

e) contacts with a person who has been or is currently engaged in activities aimed against interests of the Czech Republic;

f) sentence imposed upon a final and conclusive judgment;

g) providing of false or misleading information or omission of material information for unbiased determination of facts of the case during the procedure according to Part four of this Act, or not reporting changes to data listed in the annex to this PSC application (S. 94) or in other material provided to the Authority in annex to this application;

h) breach of duties in protection of classified information;

i) repeated failure to provide essential cooperation during security procedure initiated according to S. 101 par. 1; or

j) conditional discontinuance of criminal prosecution for intentional offence or conditional postponement of submission of motion to sentencing for intentional offence, in cases of which the prescribed probationary period has not expired yet, or approval of settlement in case of intentional criminal act.

(4) In case of an application according to S. 94, security risks outlined in paragraphs 2 and 3 a) will be investigated for a period starting at applicant's 15 years of age; investigation of security risks outlined in paragraphs 3 b) to i) shall cover the last 10 years from the date of submission of application for the security classification level CONFIDENTIAL, 15 years for the security classification level SECRET and 20 years for the security classification level TOP SECRET, or the period shall be covered from the applicant's 15 years of age, whichever is shorter.

(5) The security risk outlined in paragraph 3 b) shall not be considered to be a security risk if the natural person had used another identity for legal reasons.

(6) The following factors shall be considered in evaluation of whether the fact outlined in paragraph 3 constitutes the security risk – the extent to which it can affect capability to maintain confidentiality of information, whether the event was or was not recent, its extent, the character and conduct of the natural person over a period specified in paragraph 4.

26.

(7) In evaluation of security risks the Intelligence Service can carry out physiodetection examinations of its members, employees and job or service candidates.

27.

28.

29.

30.

31.

32.

33.

34.

35.

CHAPTER III

Industrial security

Conditions for access of the facility to classified information and forms of access of the facility to classified information

Section 15

36. The facility, which necessarily needs access to classified information in order to perform official tasks or services may be granted access

37.

a) to classified information at the security classification level RESTRICTED under the following conditions

   1. the facility must prove by written declaration its ability to secure the protection of classified information (hereinafter reffered to as „Statement of Facility“), or
   2. the facility is a holder of a valid Facility security clearance (hereinafter referred to as „FSC“)

b) to classified information at the security classification level CONFIDENTIAL and above if the facility is a holder of a valid FSC (S. 54) for the appropriate security classification level, save as otherwise provided for in this Act (S. 58 to 62).

38.

Section 15a

Statement of Facility

(1) The facility is authorized to make a Statement of Facility, if

a) appropriate conditions have been established for the protection of classified information at the security classification level RESTRICTED, equivalent to the form of access to such information (S. 20) and to the corresponding form of securing its protection (S. 5);
b) responsible person is a holder of the Notice, PSC or Certificate.

(2) Fulfilment of conditions for access to classified information according to S. 15 bullet a) N.1 shall be proved to the provider of classified information at the security classification level RESTRICTED (hereinafter referred to as „provider of restricted information“) by the facility by handing over the Statement of Facility prior to the initial access to this information; the provider is authorized to require security documentation of the facility. Provider of restricted information will send a copy of the Statement of Facility to the Authority without delay.

(3) Facility, which will act only as originator of the classified information at the security classification level RESTRICTED, will send the Statement of Facility to the Authority without delay after its making.

(4) Facility terminating access to classified information at the security classification

level RESTRICTED shall notify in writing of this fact without delay bodies to which the Statement of Facility was handed over or sent according to par. 2 or 3; this obligation does not apply if validity of the Statement of Facility expires according to par. 5 a).

(5) Validity of the Statement of Facility terminates or expires in following cases

a) 5 years have passed after the date it was made;
b) on the day of delivery of a written notification of the facility according to par. 4 to the provider of restricted information or to the Authority;
c) on the day of delivery of the Facility Security Clearance;
d) upon dissolution or cessation of existence of the facility;
e) if the facility no longer meets any of the conditions stated in par. 1; or
f) by the change of any of the data or information stated in the Statement of Facility.

(6) The facility shall notify without delay in writing the fact of termination of validity of the Statement of Facility according to par. 5 c) to f) bodies to which the Statement of Facility was handed over or sent according to par. 2 or 3.

(7) Elements of the Statement of Facility shall be stated by the implementing legal regulation.

Section 16

Conditions for issuance of the Facility Security Clearance

(1) Facility Security Clearance (the FSC) will be issued by the Authority to the facility

a) which is economically stable;
b) which is reliable in terms of security;
c) which is able to secure the protection of classified information;
d) if the responsible person is a holder of valid PSC at least for such security classification level for which the facility applies in its application for issuance of FSC;
e) which reimbursed at the time of submission of the application for issuance of FSC the administration fee according to another legal regulation.

(2) Conditions outlined in paragraph 1 a) to d) shall be fulfilled by the facility until the expiration of the FSC (S. 55).

Section 17

Economic stability

(1) The condition of economic stability will not be fulfilled by the facility

a) on which moratorium was introduced by court;
b) towards the property of which a decision on bankrupcy was issued;

c) in case of which compulsory administration was imposed.

(2) The facility can also be considered to be unstable as far as the economic stability is concerned

a) which has registered arrears in tax records kept by the Tax Administration Office of the Czech Republic or by the Customs Administration of the Czech Republic, with the excpetion of arrears where deferrement is allowed to pay off arrears or payment by installments;
b) which constantly or repeatedly does not fulfill financial obligations towards the state, natural or legal persons; or
c) in case of which the decision to distrain property was made.

Section 18

Security reliability

(1) The condition of security reliability will not be fulfilled by the facility, which was ascertained to bear a security risk.

(2) Security risk is considered to be

a) activity of an authorized representative or its member, of a member of a control body or a proctor against the interests of the Czech Republic;
b) activity of an authorized representative or its member, of a member of a control body or a proctor, consisting in supressing of human rights and freedoms, or supporting such activities;
c) the fact that the facility is a joint stock company having the form of bearer stocks in a different form than registered shares;
d) the fact, that the partner with crucial influence on choise or appointment of the authorized representative or of a control body of the facility, is a joint stock company having the form of bearer stocks in a different form than registered shares.

(3) Also the following may be considered to be a security risk

a) providing false information or concealment of a material information necessary for objective and full determination of facts of the case during the procedure of verifying conditions for issuance of the FSC, or omission to report changes to data listed in the application according to S. 96 or in other material provided to the Authority with respect to this application;
b) capital, financial or commercial relations with other natural or legal persons or with a foreign power engaged in activities aimed against the interests of the Czech Republic;
c) personal instability of the authorized representative or of the control body or with respect to persons of proctors;
d) breach of obligations in the protection of classified information;
e) final and conclusive conviction of an intentional offence of the natural person who is a partner of the facility;

f) intentional breach of legal regulations by the partner of the facility, by the member of cooperative association or by other person who has crucial influence on choice or assignment of the authorized representative or control body of the facility or cooperative association, or activities of above mentioned subjects against the interests of the Czech Republic;
g) intentional breach of legal regulations by individuals authorised to act on behalf of or for the facility that could cause damage to the interests of the Czech Republic;
h) relations of a person, who has influence on actions and conduct of the facility on the basis of labour-law, member or other contractual relationship, to natural persons or legal persons or to foreign power, which have been or are currently engaged in activities aimed against the interests of the Czech Republic;
i) repeated non-providing of needed cooperation during procedure initiated according to S. 101 par. 1; or
j) final and conclusive conviction of an intentional offence concerning the facility.

39.

(4) Crucial influence resulting from par. 2 d) and par. 3 f) is the possibility to enforce effectively or on the basis of the law the appointment, discharge from position or choice of a person who is an authorized representative, or of the majority of persons, who are members of the authorised representative or members of the control body of the facility or of the cooperative association. Influence resulting from par. 3 h) is the posibility to have influence on activities of the facility by means of rules governing that facility.

Section 19

Eligibility to secure the protection of classified information

40. The condition of eligibility to secure the protection of classified information will not be fulfilled by the facility, which is not able to ensure and comply with respective forms of securing protection of classified information according to this Act with respect to the corresponding security classification level and to the form of access to classified information.

41.

42.

43. **Section 20**

44.

45. **Form of access of the facility to classified information**

46.

(1) The facility has access to classified information that

a) is originated by or released to the facility; or
b) is not originated by or released to the facility, but is accessible by persons acting on behalf of or for the facility, in connection with performance of work or other activities for the facility on the basis of a contract.

(2) In case of access according to paragraph 1 b), the facility shall fulfill the condition according to the S. 16 par. 1 c) only by ensuring the protection of classified information based on personnel security [S. 5 a)].

47.

CHAPTER IV

48. **Administrative security**

49.

50. **Markings and records of classified information**

51.

52. **Section 21**

53.

(1) Information that complies with elements according to S. 4 and that is included in the list of classified information shall be marked by the originator with the name of the originator, security classification level of the information, its registration mark and date of its creation, save as otherwise provided herein.

(2) Classified information provided to the Czech Republic by a foreign power shall be marked with the security classification level in accordance with S. 4 by a State body, legal person or natural person pursuing business, if they are the first ones to register this classified information (S. 77 to 79), in accordance with international agreement by which the Czech Republic is bound and on the basis of which the classified information is released, including relevant abbreviations according to this agreement (for example EU, EURO or NATO), or as prescribed by the foreign power or in accordance with the security classification level marked on the released classified information by the foreign power; the name of the originator and the date of creation of classified information will not be marked.

(3) The relevant additional marking shall also be applied to the category information, which requires more stringent conditions for providing different types of protection of classified information (hereinafter referred to as "Special Handling Regime") in the areas determined in particular by international agreement, by which the Czech Republic is bound, or determined by regulations of an international organization, of which the Czech Republic is a member (for example the term "CRYPTO" in case of information from the area of cryptographic protection, and the term "ATOMAL" in case of information from the area of mass destruction weapons).

(4) If the marking according to par. 1 to 3 cannot be applied to the information, it shall be stated in such a form that it is possible to determine the necessary details at any time.

(5) Classified information shall be registered in administrative aids specified by the implementing legal regulation and as described therein; this does not apply if in case of source materials classified as RESTRICTED the responsible person has added to classified information at the security classification level RESTRICTED that these do not have to be registered. Also handing over, receiving or other transfers of classified information shall be registered in administrative aids.

(6) Reproductions, copies or translations of classified information at the security classification level TOP SECRET or extract from this information may be produced only upon the written consent of the originator; in case of classified information at security classification levels SECRET or CONFIDENTIAL they may be produced only upon the written consent of the directly superior officer.

(7) Classified information may be transported or carried only in portable containers or in closed package depending on its security classification level and on its carrier; it can be transported only by courier service or by postal service licence holders.

(8) Receipt of classified information shall be acknowledged by the recipient, save as otherwise provided for in this Act (S. 23 par. 1).

(9) In the course of a destruction period prescribed according to a special legal regulation classified information may be lent only to such natural persons who are towards the State body, legal person or natural person pursuing business in a service relationship or a labour-law relationship, a member relationship or in a similar relationship.

(10) During the procedure aimed at safe destruction of classified information in the process of removing of classified information the procedure shall be in accordance with a special legal regulation.

Section 22

(1) The security classification level shall be marked on the classified information at the time of its creation by its originator, save as otherwise provided for in this Act (S. 70).

(2) Security level markings of the classified information shall be maintained throughout the duration of reasons for confidentiality. The security classification level shall not be changed or declassified without the consent of the originator or of the releasing foreign power.

(3) If necessary with respect to the nature of the classified information, the originator shall mark on this classified information the period for which it shall be kept secret; the security classification level will expire on the marked date.

(4) The security classification level shall be immediately changed or the information shall be declassified by the originator, if it was ascertained that the reason for classification of information ceases to exist, that the reason for classification does not correspond to the stipulated security classification level or if the classification level has been determined unwarrantedly, and this declassification or new classification level shall be marked by the originator on the corresponding classified information.

(5) The originator shall verify whether the reason for confidentiality of information still applies and he/she/it shall review it no less frequently than every 5 years from the date of its creation.

(6) If the originator changed or declassified the security classification level according to paragraph 4, he/she/it shall inform immediately in writing all addressees of this classified information. Addressees of this classified information shall inform immediately in writing all other addressees authorised by them to have access to this classified information.

(7) The addressee shall mark declassification or change of the classification level of the classified information after notification of the change or declassification according to paragraph 6.

(8) In case of termination of the existence of the originator the declassification or change of the security classification according to paragraph 4 and notification according to paragraph 6 shall be performed by its legal successor, in case there is no such legal successor

or if the legal successor does not comply with conditions regulating access to classified information, then this responsibility shall be assumed by the Authority.

Section 23

54.

(1) If classified information requiring Special Handling Regime is not in question, the duty outlined in S. 21 par. 8 does not apply to the transfer of classified information

a) up to the security classification level SECRET between the Intelligence Services and similar services of a foreign power, conducted within the framework of cooperation according to the special legal regulation, in the cases, when the procedure according to S. 21 par. 8 cannot be complied with;
b) at the security classification level RESTRICTED, if determined so by the responsible person and if the foreign power or the originator of the classified information do not explicitly require to sign and acknowledge its handing over or transmission.

(2) The implementing legal regulation shall determine

a) the method of marking elements on classified information according to S. 21 par. 1 to 4, and S. 22 par. 1, 3, 4 and 7, particularly in connection to the security classification level of the classified information and to the carrier of the classified information;
b) the types of administrative aids outlined in S. 21 par. 5, particularly in the form of books, workbooks or sheets, their elements and organizational and technical requirements for their maintaining, and the extent of source materials at the security classification level RESTRICTED for the classified information at the security classification level RESTRICTED;
c) the elements of the consent to make reproductions, copies, extracts and translations of the classified information (S. 21 par. 6), the method of necessary markings on these information and the method of making of extracts;
d) details concerning transport, handing over, transmission, receipt and lending of classified information according to S. 21 par. 7 to 9 and details concerning subsequent handling of classified information relating to above mentioned activities, including organizational securing of these activities, requirements for portable containers and packages and marking of relevant elements on them, particularly in connection with the security classification level of the classified information and with the carrier of classified information.

(3) Provisions of this Chapter do not relate to processing and transmission of classified information in information systems and cryptographic devices.

(4) The Authority will notify in the Collection of Laws of the Czech Republic conversion tables of the classification levels according to the international contracts, by which the Czech Republic is bound.

CHAPTER V

55. Physical security

57. **Section 24**

(1) Within the framework of physical security, premises, security areas and meeting areas shall be determined for ensuring the protection of classified information.

(2) Premises means a building or another limited area, where security area or meeting areas are usually situated.

(3) The security area means a limited area within the boundary of the premises.

(4) The meeting area will be a location within the boundary of the premises. Classified information at the security classification levels TOP SECRET or SECRET may be regularly discussed only within the meeting area.

(5) Classified information shall be processed

a) in the security area of the appropriate category or above;
b) within the premises of the appropriate category or above, on condition that it is ensured that unauthorised individuals are denied access to classified information;
c) in justified cases with the written consent of a responsible person or a security officer within the premises of a different category than appropriate for the security classification being processed, on condition that it is ensured that unauthorised individuals are denied access to classified information; or
d) in justified cases with the written consent of a responsible person or a security officer outside the premises, on condition that it is ensured that unauthorised individuals are denied access to classified information.

(6) Classified information shall be stored in the security area of the appropriate category or above and within this area in a security container, lockable cabinet or in other security container, if necessary, under the conditions determined by the implementing legal regulation.

Section 25

(1) According to the highest classification level of classified information being stored in security areas and according to the highest classification level of classified information being processed in premises, security areas/premises will be categorized as follows

a) TOP SECRET;
b) SECRET;
c) CONFIDENTIAL; or
d) RESTRICTED.

(2) According to the possibility to have access to classified information security areas will be categorised into the following classes

a) Class I, the entry into the Class I area constitutes access to classified information;

b) Class II, the entry into the Class II area does not constitute access to classified information.

(3) Entry into and exit from the security area shall be controlled by measures according to S. 27. Unauthorised person may enter only security area of Class II and if accompanied by a person authorised to enter this area.

(4) In justified cases, with written consent of the responsible person or with the written consent of a person authorized by the responsible person Class I can be changed to Class II for a necessary period of time if the state and conditions are secured, that no unauthorised person has access to classified information.

Section 26

Discussions involving classified information

(1) The responsible person shall ensure that in the meeting area according to S. 24 par. 4, classified information is not threatened and no leakage of classified information is possible.

(2) In order to meet the requirements according to paragraph 1, the responsible person shall ask the Authority to carry out the technical security examination of an unauthorised use of technical devices intended to obtain data within the meeting area. The responsible person may ask for such examination also in case of security areas categorised as SECRET or TOP SECRET. This examination shall be ensured by the Authority in cooperation with the Intelligence Services and the Police of the Czech Republic (hereinafter referred to as "the Police"). For their own needs, the Intelligence Services and the Police carry out the examination independently.

(3) Entry into and exit from the meeting area shall be controlled by measures according to S. 27. Unauthorised person may have access to the meeting area only if accompanied by a person who is authorised to access to this area.

Section 27

Measures of the physical security are as follows

a) guarding;
b) special handling measures;
c) technical means.

Section 28

(1) Continuous security guarding shall be ensured at premises housing the security area, depending on its categories as follows

a) TOP SECRET, at least two persons at the premises;

b) SECRET, at least one person at the premises and one other person who shall be able to take quick action upon alarm annunciation by technical means if carrying out of the protection of classified information is breached/violated;
c) CONFIDENTIAL, at least one person who shall be able to take quick action upon alarm annunciation by technical means if carrying out of the protection of classified information is breached/violated.

(2) In the case of premises housing the security area of the category no higher than RESTRICTED and in the case of premises without security area or meeting area, guarding will be provided to the extent decided by the responsible person.

(3) In case of premises housing the meeting area, where classified information at the security classification level TOP SECRET is regularly discussed, guarding shall be ensured at least by 2 persons at the premises. In the case of premises housing the meeting area, where classified information at the security classification level SECRET is regularly discussed, guarding shall be ensured by 1 person at the premises and 1 other person, who shall be able to take quick action upon alarm annunciation by technical means if carrying out of the protection of classified information is breached/violated.

(4) Guarding shall be secured by employees of the State body, of the legal person or by employees of the natural person pursuing business in their respective premises, by members of armed forces or armed security corps of a foreign power or by employees of the Security protection service.

Section 29

Authorization of persons and vehicles to enter and exit the premises, authorization of persons to enter the security area and the meeting areas and the method of control of these authorizations, as well as methods of handling keys and identification means, which are used for systems of entry safeguarding according to S. 30 par. 1 b), and the method of handling technical means and their use shall be determined by special handling arrangements. The special handling arrangements shall also determine authorizations for exit of individuals and vehicles from the premises and for their control, as well as conditions and methods of control of movement of persons within the premises, security area and meeting area and the method of control and removal of classified information from the premises, security area and meeting area.

Section 30

(1) Technical means shall be in particular

a) mechanical barrier devices;
b) electrical locking mechanisms and entry control systems;
c) electrical safeguarding signalling devices;
d) special television systems;
e) emergency systems;
f) electrical fire detection devices;
g) devices for physical searches of dangerous substances or objects;

h) devices for physical destruction of information data carriers;
i) devices impeding passive and active eavesdropping of classified information.

(2) Marks score (S. 31 par. 1) will be assigned to certified technical means [S. 46 par. 1 a)] and to uncertified technical means approved by the responsible person or by a person authorized by the responsible person.

(3) In the case of engagement of the Czech Republic in international armed conflict, international rescue or humanitarian action, in other missions abroad, in cases of declaration of belligerency, in case of state of danger, emergency or endangering of the State, in case of intelligence operations of the Intelligence Services as well as during activities of the Armed Forces of the Czech Republic within the frame of military exercise and practical military training using military technology and military equipment outside permanent dislocation places of the army unit, the technical means listed in paragraph 1 may be replaced by intensified security guarding at a higher level than that outlined in S. 28, which will be carried out by the armed forces staff or by armed security corps staff on the basis of the special legal regulations or by members of armed forces of a foreign power.

Section 31

(1) Level of safeguarding of the meeting area and of the security area by the physical security measures shall be determined by marks score of these measures depending on the risk assessment; marks score and the lowest level of safeguarding shall be determined by the implementing legal regulation.

(2) Measures of the physical security or combination of more of these measures must correspond at least to the lowest level of safeguarding of the meeting area and of the security area and these measures shall be determined with respect to risks assessment and to the security classification level of information being regularly discussed in the meeting area, or to the category of the security area.

(3) Measures stated in paragraph 2 and measures realating to the physical security of the premises without security area or meeting area shall be approved and determined by the responsible person or by a person authorized by the responsible person in the physical security project.

(4) Assessment of risks shall be carried out continuously and the level of physical security measures shall be adjusted, as necessary.

(5) The State body, legal entity and natural person pursuing business shall ensure and periodically review whether physical security measures being used correspond to the physical security project and to legal regulations in the area of protection of classified information.

58.
59. **Section 32**
60.
61. **Physical security project**
62.

(1) In case of premises housing security areas categorized as TOP SECRET, SECRET or CONFIDENTIAL the following shall be involved in the physical security project

a) determination of premises and security areas, including their perimeters and determination of categories and classes of security areas;
b) risks assessment;
c) method of application of physical security measures;
d) operating rules of the premises;
e) emergency plan of safeguarding of premises and security areas.

(2) In case of premises housing only security areas categorizsed as RESTRICTED the following shall be involved in the physical security project

a) determination of premises and security areas, including their perimeters and determination of categories and classes of security areas;
b) method of application of physical security measures.

(3) In case of premises housing the meeting area the following shall be involved in the physical security project

a) determination of premises and determination of the meeting area, including their perimeters;
b) risks assessment;
c) method of application of physical security measures;
d) operating rules of premises;
e) emergency plan of safeguarding of premises and of the meeting area.

(4) In case of premises categorized as TOP SECRET, SECRET and CONFIDENTIAL without security area or meeting area the following shall be involved in the physical security project

a) determination of premises, including its perimeters;
b) method of application of physical security measures;
c) operating rules of premises and
d) emergency plan of safeguarding of premises.

(5) In case of premises categorized as RESTRICTED without security area the physical security project shall contain determination of premises, including its perimeters.

(6) In cases according to the Section 30, par. 3, provisions of paragraphs 1 to 5 shall be applied accordingly for the physical security project; the extent of the project shall be approved and determined by the responsible person or by a person authorized by the responsible person.

(7) The physical security project shall be deposited with the responsible person or with the security officer.

Section 33

Delegating provisions

The implementing legal regulation shall determine

a) the method of storing classified information depending on the level of its security classification (S. 24 par. 6);
b) organizational requirements for guard operations (S. 28) and safeguarding of the meeting area or security area by this guard, including determination of the category of individuals listed in S. 28 par. 4, depending on the security classification level of classified information that is regularly discussed in the meeting area, on the category of premises or on the category of the security area;
c) details of special handling requirements (S. 29);
d) requirements for technical means listed in S. 30 par. 1, and safeguarding of premises, meeting area or security area by these means, depending on the security classification level of classified information that is regularly discussed in the meeting area, or on the category of the security area or on the category of premises;
e) the marks score of individual physical security measures and marks score of the lowest level of safeguarding of the meeting area or security area, including the basic method of the risks assessment (S. 31 par. 1 and 2);
f) the frequency and method of records concerning verification whether the used physical security measures conform with the physical security project and with legal regulations in the area of protection of classified information, depending on the security classification level of classified information (S. 31 par. 5);
g) the content of operating guidelines of premises and content of the emergency plan for safeguarding of premises, security areas and meeting areas [(S. 32 par. 1 d) and e) and S. 32 par. 3 d) and e)].

CHAPTER VI

63. **Information and communication systems security**

64.

65. **Section 34**

66.

67. **Information system**

68.

(1) For the purpose of this Act the information system handling classified information will consist of one or more computers, their software, connected peripherals, administration of this information system, together with associated processes or devices able to collect, create, process, store, display or transmit classified information (hereinafter “the Information System”).

(2) The Information System must be certified by the Authority [S. 46 par 1b)] and approved for operation in writing by the responsible person or by a person authorized by the responsible person.

(3) Information system of the facility with access to classified information classified as RESTRICTED may be approved for operation only when the Statement of Facility is valid; expiration of validity of the Statement of Facility shall entail expiration of the approval of the information system for operation.

(4) Classified information may be handled only in the Information System that fulfils conditions according to paragraph 2 or 3.

(5) Approval for operation of the Information System according to paragraph 2 must be notified by the responsible person or by a person authorized by the responsible person to the Authority in writing within 30 days of this approval.

(6) The implementing legal regulation shall determine

a) requirements for the Information System and conditions of its secure operating depending on the security classification level of classified information handled by the system and on the security operation mode; and
b) content of the Information System security documentation.

Section 35

Communication system

(1) For the purpose of this Act the communication system handling classified information (hereinafter "the Communication System") shall be a system ensuring the transmission of this information between end-users, and involving communication terminals, transmission environment, encryption means, operators and operational conditions and procedures.

(2) The Communication System shall not be operated without the project of Communication System security approved by the Authority. The approval of the project of the Communication System security shall be required from the Authority by the State body, legal person or natural person pursuing business who will operate it.

(3) Classified information may be handled only in the Communication System that meets conditions according to paragraph 2.

(4) Communication System shall be approved for operation in writing by the responsible person or by a person authorized by the responsible person.

(5) Communication System of the facility with access to classified information classified as RESTRICTED may be approved for operation only when the Statement of Facility is valid; expiration of validity of the Statement of Facility shall entail expiration of the approval of the Communication System for operation.

(6) Implementing legal regulation shall determine

a) the content of the application for approval of the project of Communication System security; and
b) the elements of the project of Communication System security and methods and conditions for its approval.

Section 35a

Handling of tactical information

(1) For the purposes of this Act the tactical information shall mean classified information with a reason for a short time justifying its classification. Tactical information shall be handled in Information or Communication Systems and during its transmission it shall be safeguarded by means of cryptographic protection.

(2) The protection of tactical information up to the security classification level SECRET may be ensured also by the set of measures determined on the basis of risks assessment. Conditions of different way of handling of tactical information are specified by the security standard.

CHAPTER VII

69. Protection of classified information during handling in electronic form in the device, which is not a part of Information or Communication Systems

Section 36

(1) Concerning classified information being handled in electronic form in the device, which is not a part of Information or Communication Systems, in particular in memory typewriters and in machines allowing copying, recording or display of classified information or its transmission to another data format, the protection of this classified information shall be ensured.

(2) The State body, legal person and natural person pursuing business shall issue security operation guidelines for any device listed in paragraph 1 and being operated by them; classified information may be processed only in accordance with these guidelines.

(3) In the security operation guidelines according to paragraph 2 the following stall be stated for the device according to paragraph 1

a) the method of its secure operation;
b) operation guidelines for its user.

(4) Conditions of the secure operation of the device listed in paragraph 1, depending on the security classification level of classified information being processed by it, shall be determined by the implementing legal regulation.

CHAPTER VIII
Cryptographic protection

Section 37

(1) Cryptographic material means cryprographic device, material to ensure its function or cryptographic document.

(2) Cryptographic devices used for the cryptographic protection of classified information shall be certified by the Authority [S. 46 par. 1c)]

(3) Cryptographic site means a site for production or testing of the material determined to ensure the function of the cryptographic device, to store the cryptographic material or to distribute and record cryptographic material or to produce and test cryptographic devices. The cryptographic site must comply with security standards and shall be subject to approval by responsible person or by security officer prior to live activation.

(4) The cryptographic site, which is determined for production or testing of the material for providing the function of the cryptographic device or which is distribution and registration centre of cryptographic material of the State body, legal persons or natural persons pursuing business, must be certified by the Authority prior approval to live activation by the responsible person or by the security officer [S. 46 par. 1d)].

(5) A State body, legal person or natural person pursuing business that carry out cryptographic protection shall keep records of cryptographic material, cryptographic protection staffs, operators of cryptographic devices and couriers of cryptographic material.

Section 37a

Controlled cryptographic item

(1) The controlled cryptographic item shall be unclassified device or its part included in the list according to paragraph 3 designated to protect information during its processing or transmission and using cryptographic methods.

(2) Controlled cryptographic item can be used only in accordance with the security standard.

(3) The device outlined in paragraph 1 or its part will be approved by the Authority upon written request of its producer, importer, distributor or user and put on the list of controlled cryptographic items kept by the Authority if this is in accordance with intents of the Czech Republic in the area of securing of protection of classified information.

Section 38

Performance of cryptographic protection

(1) The performance of cryptographic protection means

a) its security administration;
b) specific operation of a cryptographic device; or
c) production of cryptographic device or material to ensure its function.

(2) The performance of cryptographic protection shall be the task of the cryptographic protection officer who is

a) charged with the cryptographic protection by the responsible person or by a person authorized by the responsible person;
b) a holder of valid PSC and
c) a holder of a certificate of a specific specialist competence of the cryptographic protection officer (hereinafter "the Specialist Competence Certificate").

Section 39

70.

71. **Specific specialist competence of a cryptographic protection officer and a specific specialist competence exam**

(1) Specific specialist competence of a cryptographic protection officer (hereinafter "the Specific Specialist Competence") comprises the knowledge of regulations from the area of cryptographic protection of classified information, ability of their application and other abilities according to S. 38 par. 1. This knowledge and abilities shall be verified by the Authority by a specific specialist competence exam (hereinafter „the Specialist Exam"). The Specialist Exam will be passed at the board of examiners; this is not condition for its part taken according to paragraph 3 b). Members of the board of examiners will be designated by the responsible person or by a person authorized by the responsible person to the Authority or to the State body according to paragraph 3 a). Those who passed the Specialist Exam will be issued with the Specialist Competence Certificate according to paragraph 3 a) by the Authority or the State body, which shall keep records of this. The Specialist Competence Certificate will be issued for a maximum period of 5 years.

(2) An application for a Specialist Exam shall be submitted in writing by the responsible person of the State body or of the facility with the Authority or with the State body delegated by the Authority. The Specialist Exam shall be passed within 6 months from the date of submission of application. The Authority or the State body delegated by the Authority shall notify in writing the individual who submitted the Specialist Exam application of the date and place of the Specialist Exam; the notification shall be sent 20 days prior to the date of exam at the latest. Any person who fails an exam may repeat it. The repeated exam can be taken only after 5 working days from the date of an unsuccessful exam.

72.

(3) A contract for providing activities according to S. 52 can be made by the Authority with the State body, the subject-matter of the contract will be

a) taking of the Specialist Exam and issuance of Specialist Competence Certificate; or
b) taking of a part of the Specialist Exam concerning S. 38 par. 1b) or c) and corresponding relationship to S. 38 par. 1a). The Authority can make the contract according to bullet b) also with the facility.

Section 40

Operation of the cryprographic device

(1) Operation of the cryptographic device means performance of user functions of the cryptographic device.

(2) Operators operating the cryptographic device according to paragraph 1 shall

a) be entrusted with the operation by the responsible person or by the person authorized by the responsible person;
b) meet conditions for access to classified information according to S. 6 par. 1 or S. 11 par. 1; and
c) be trained to be able to operate the cryptographic device.

Section 41

Manipulation of cryptographic material and controlled cryptographic item

(1) Manipulation of cryptographic material means the form of transmission, transportation,
lending, storing or another manner of handling of cryptographic material including discarding of it.

(2) Cryptographic material may be recorded and handled only in a manner and by means ensuring the protection of the cryptographic material and fulfilling requirements determined by the implementing legal regulation.

(3) The protection of cryptographic device and material to ensure its function up to classification level CONFIDENTIAL without the need of their storing may be provided in a manner ensuring that the cryptographic device and material will be under permanent control of their authorized user.

(4) Controlled cryptographic item can be registered, processed, stored, transported, exported, controlled and distributed in a manner ensuring its protection and fulfilling requirements of the security standard.

Section 42

Transportation of cryptographic material and export of cryptographic device

(1) Transportation of cryptographic material shall be carried out by a courier of cryptographic material. The courier of cryptographic material shall be the person who

a) was assigned to transport the cryptographic material by the responsible person or by a person authorized by the responsible person;
b) is a holder of valid PSC, at least at the same security classification level as that of the cryptographic material being transported;
c) was trained for the transportation.

(2) Export of the certified cryptographic device [S. 46 par. 1 c)] from the territory of the Czech Republic shall be subject to the licence of the Authority. Utilization of certified cryptographic device by the State body outside the territory of the Czech Republic will not be considered to be an export.

(3) Licence according to paragraph 2 can be granted upon written request. The licence shall be granted for export of specific cryptographic device and it shall also contain the purpose of export. No licence will be granted by the Authority if the export would endanger

classified information of the Czech Republic or classified information that the Czech Republic has undertaken to protect; the Authority shall report this fact in writting to the licence applicant. No claim can be laid to the granting of licence.

(4) The Authority shall keep records of licences granted according to paragraph 2.

Section 43

81. **Compromise of the cryprographic material**
82.

(1) Compromise of cryptographic material means such handling of cryptographic material that resulted or could result in breach of protection of classified information.

(2) Compromise of cryptographic material shall be immediately reported to the Authority by the State body, legal person or natural person pursuing business.

Section 43a

(1) Distribution and keeping records of cryptographic material of the Czech Republic, cryptographic material of the European Union and cryptographic material distributed on the basis of the international agreement, the cryptographic material for military purposes excepted, shall be ensured by the Authority. Distribution and keeping records of cryptographic material of the North Atlantic Treaty Organisation and cryptographic material for military purposes shall be ensured by the Ministry of Defence.

(2) Conditions of keeping records, handling and supervision of cryptographic material in the Czech Republic, comprising in particular possibility to establish the book of records (accounts) for cryptographic material in State bodies or facility, keeping records, control functions, duties of holders of cryptographic material with respect to the Authority or Ministry of Defence, as well as ensuring of courier services for the cryptographic material of the Euroepan Union shall be regulated by the security standard.

Section 44

Delegating provisions

83. The implementing legal regulation shall determine

a) elements of the application for the Specialist Exam;
b) organization, content and method of performance of Specialist Exam;
c) format of the Specialist Competence Certificate;
d) minimum requirements for ensuring the security administration of the cryptographic protection;
e) details of providing operation of cryptographic device;
f) method of training of operators of cryptographic device and of the courier of cryptographic material and the format of confirmation of training of the operator of the cryptographic device and of the courier of cryptographic material;

g) details of the method of marking elements on classified information from the area of cryptographic protection, particularly according to the type of the cryptographic material;
h) types and elements of administrative aids of cryptographic protection and requirements for administration of these aids;
i) detailed requirements for method and for means of handling of cryptographic material;
j) content of application for granting export licence for export of certified cryptographic devices from the territory of the Czech Republic and elements of the licence;
k) method of keeping records listed in S. 37 par. 5;
l) categories of cryptographic sites, types of operation on the cryptographic site and minimum requirements for their safeguarding;
m) conditions of protection of the cryptographic device and material to provide its function according to S. 41 par. 3.

Section 45

Compromising electromagnetic emissions

(1) Protection of classified information classified as TOP SECRET. SECRET or CONFIDENTIAL from its leakage by compromising electromagnetic emissions means securing of electrical and electronic devices, security area or premises.

(2) If the protection of classified information from leakage by compromising emissions will be provided by a shielded chamber, this chamber must be certified by the Authority [S. 46 par. 1 e)].

(3) Verification of capability of electrical and electronic devices, security area or premises to

84. protect classified information from leakage by compromising electromagnetic emissions shall be secured by the Authority during certification of Information System or of cryptographic device, during approval of the security project of Communication System or on the basis of reasonable written request from the State body or facility with regard to the protection of classified information.

85.

(4) Contract can be made between the Authority and the State body or facility according to S. 52 for taking measurements of possible leakage of classified information as outlined in paragraph 3, i.e. the contract for providing these services.

(5) The Intelligence Services are qualified to take measurements of device, security area or

86. premises as outlined in paragraph 3 that are operated or used by Intelligence Services. In these cases no contract according to S. 52 will be required. For the purpose of certification of Information System or cryptographic device or during approval of the security project of Communication System the report on the measurement taken including its results will be provided by the Intelligence Services to the Authority.

87.

(6) When conducting measurements according to paragraph 5 the Intelligence Services

shall comply with provisions of this Act, implementing legal regulations and security standards of the Authority.

CHAPTER IX

88.

89. **Certification**

90.

91. **Section 46**

92.

Common provisions

(1) Certification means the procedure whereby the Authority

a) verifies the capability of technical means to protect classified information;
b) verifies the capability of Information System to handle classified information;
c) verifies the capability of cryptographic device to protect classified information;
d) verifies the capability of cryptographic sites to perform activities according to S. 37 par. 4; or
e) verifies the capability of shielded chambers to protect classified information.

(2) If the Authority ascertains capability according to paragraph 1 it will issue a technical means certificate, information system certificate, cryptographic device certificate, cryptographic site
certificate or a shielded chamber certificate.

(3) Certificates according to paragraph 2 shall be the legal instruments.

(4) The following shall be included in the technical means certificate

a) registration number of the certificate;
b) name and type designation of the technical means;
c) identification of the technical means manufacturer by the business firm (hereinafter "the Firm") or by name, identification number of the person (hereinafter „the identification number") and by location in case of a legal person, or by name, surname, birth registration number (personal identity number) and permanent residence in case of a natural person;
d) identification of the holder of the technical means certificate according to c) above;
e) evaluation of the technical means;
f) date of issue and validity period of the certificate; and
g) official stamp and signature of the authorized representative of the Authority or, if this certificate was issued in the electronic form, electronic signature of the authorized representative of the Authority in accordance with the special legal regulation.

(5) The following shall be included in the Information System certificate, cryptographic device certificate, cryptographic site certificate and shielded chamber certificate

a) registration number of the certificate;
b) identification of the holder of the certificate according to paragraph 4 c);
c) date of issue and validity period of the certificate; and
d) official stamp of the Authority and signature of the authorized representative of the Authority or, if these certificates were issued in the electronic form, recognized electronic signature of the authorized representative of the Authority in accordance with the special legal regulation.

(6) In addition to the elements according to paragraph 5 the Information System certificate shall contain the identification of the information system and the security classification level of classified information for which the capability of the Information System has been verified.

(7) In addition to elements according to paragraph 5 the cryptographic device certificate shall contain

a) identification of the cryptographic device;
b) identification of the cryptographic device manufacturer according to paragraph 4 c); and
c) security classification level of classified information for which the capability of the cryptographic device has been approved.

(8) In addition to elements according to paragraph 5 the cryptographic site certificate shall contain

a) identification of the cryptographic site;
b) scope of capability of the cryptographic site; and
c) category of the cryptographic site.

(9) In addition to elements according to paragraph 5 the shielded chamber certificate shall contain

a) identification of the shielded chamber for which it has been issued;
b) identification of the shielded chamber manufacturer according to paragraph 4 c); and
c) security classification level of classified information for which the capability of the shielded chamber has been approved.

(10) If the Authority is not satisfied concerning the capability according to paragraph 1, it shall determine that the certificate will not be granted. No appeal shall be permitted against the decision not to grant a certificate according to paragraph 1 b) and c).

(11) The Authority shall decide the termination of validity of the certificate in cases outlined in S. 47 par. 4 b), S. 48 par. 4 d), S. 49 par. 5 b), S. 50 par. 4 d) and S. 51 par. 4 d). An appeal lodged against the decision of the Authority to terminate validity of the certificate has no suspension effect. No appeal shall be permitted against the decision of the Authority to terminate validity of the Information System certificate and cryptographic device certificate.

(12) If validity of the certificate expired or was terminated according to S. 47 par. 4 b), S. 48 par. 4 b) and d), S. 49 par. 5 b), S. 50 par. 4 b) and d), or S. 51 par. 4 b) and d), the

certificate holder shall forward the certificate to the Authority, within 5 days from the date of delivery of the decision of the Authority.

(13) The certification report shall be the Annex of Information System certificate, cryptographic device certificate, cryptographic site certificate or shielded chamber certificate that shall contain principles and conditions for their operation. Conditions of the use of technical means may be set forth in the Annex of the technical means certificate.

(14) The Authority shall verify capability of the technical means according to paragraph 1 a) on the basis of evaluations of technical means parameters (hereinafter "the Evaluations").

(15) The Authority can conclude a contract with the State body or with the facility according to S. 52 for purposes of issuing Evaluations according to paragraph 14 and for purposes of performance of partial tasks in verifying capability according to paragraph 1 b) to e); this possibility does not apply to the cases of verification of capability of Information Systems, cryptographic devices or cryptographic sites or shielded chambers intended to be used by the Intelligence Services.

(16) The list of the State bodies and facilities, with which the Authority concluded a contract according to S. 52, will be published by the Authority in the Bulletin of the Authority.

(17) Only the Intelligence Services concerned are authorized to perform partial tasks in verifying capability according to paragraph 1 b) to e) that cannot be performed by the Authority for reasons of confidentiality, where Information Systems, cryptographic devices, cryptographic sites or shielded chambers are in question, that are intended to be used by these Intelligence Services. In these cases reports shall be forwarded to the Authority by the Intelligence Services on performance of partial tasks, including results.

(18) In performing partial tasks according to paragraph 17 the Intelligence Services shall comply with provisions of this Act, implementing legal regulations and security standards of the Authority.

(19) The requesting subject according to S. 47 par. 1, S. 48 par. 1, S. 49 par. 1, S. 50 par. 1 and S. 51 par. 1 shall be the party of the certification procedure or of the certificate revoking procedure.

Section 47

93. Request for technical means certification and validity of the technical means certificate

(1) A technical means certification shall be requested in writing with the Authority by the producer, importer, distributor or user of the technical means. Evaluations according to S. 46 par. 14 and the documentation necessary to carry out the technical means certification shall be enclosed in the request.

(2) The validity period of the technical means certificate shall be determined by the Authority for the period not exceeding 5 years.

(3) The list of certified technical means will be published in web sites of the Authority, with the exception of technical means certified upon request of the user of technical means.

(4) Validity of the technical means certificate shall terminate

a) upon expiration of its validity period; or
b) by decision of the Authority on termination of the certificate validity if the technical means being produced fails to comply with requirements of this Act and of implementing legal regulations or if it is not identical to the technical means being evaluated.

(5) If validity of the technical means certificate was terminated as outlined in paragraph 4, the Authority will remove this technical means from the list published in accordance with paragraph 3.

(6) The technical means used for the protection of classified information may continue to be used even after expiration of its certificate validity period.

(7) During the process of the technical means certification, the certificate or similar document of the technical means issued by authorized professional department of the foreign power can also be taken into account by the Authority.

Section 48

94. **Request for Information System certification and validity of the Information System certificate**

(1) Information system certification shall be requested in writing with the Authority by the State body or by the facility that will operate the Information System.

(2) During the process of certification, a subject that requested for the Information System certification according to paragraph 1 shall submit all documents necessary for carrying out certification, at the request of the Authority.

(3) The validity period of the Information System certificate shall be determined by the Authority. Depending on the security level the validity of the information system certificate shall not extend beyond

a) 2 years for TOP SECRET and SECRET;
b) 3 years for CONFIDENTIAL; and
c) 5 years for RESTRICTED.

(4) Validity of the Information System certificate shall terminate

a) upon expiry of its validity period;
b) in case of Information System designated for handling classified information classified at levels CONFIDENTIAL or higher upon termination of validity of

the FSC;

c) upon dissolution of the State body;

d) by decision of the Authority on termination of the certificate validity if the Information System ceased to be serviceable for handling classified information; or

e) through notification of the State body or facility as holders of the certificate of termination of the Information System.

(5) Where the Information System is also to be used immediately after expiration of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide certification of the Information System. Repeated request shall be forwarded to the Authority at least 6 months before the expiration of a validity period of the original Information System certificate.

(6) The Authority shall take a decision on Information System certification within 1 year of initiation of the certification process, in case of more complex cases within 2 years; if the case cannot be decided within this period with respect to its nature, the director of the Authority may reasonably extend the period, but not by more than 6 months.

Section 49

Request for cryptographic device certification and validity of the cryptographic device certificate

(1) Cryptographic device certification shall be requested in writing with the Authority by the producer, importer, distributor or user of the cryptographic device. If the facility requests cryptographic device certification, it shall be a holder of the valid FSC for access to classified information according to S. 20 par. 1 a).

(2) The Authority shall reject the request according to paragraph 1 by its decision if it is not in line with intentions of the Czech Republic in the area of providing protection of classified information by cryptographic protection. No appeal shall be permitted against the decision according to the first sentence and this decision cannot be re-examined by the court.

(3) The subject that requested the cryptographic device certification according to paragraph 1, shall submit during the process of certification the necessary number of units of cryptographic device, as well as the documentation necessary for carrying out the certification, at the request of the Authority.

(4) The validity period of the cryptographic device certificate shall be determined by the Authority for the period not exceeding 5 years.

(5) Validity of the cryptographic device certificate shall terminate

a) upon expiry of its validity period; or

b) by decision of the Authority on termination of the certificate validity if the cryptographic device ceased to be serviceable for the protection of classified information.

(6) Where the cryptographic device is also to be used immediately on the expiry of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide certification of the cryptographic device. Repeated request shall be forwarded to the Authority at least 6 months before the expiration of a validity period of the original cryptographic device certificate.

(7) During the process of cryptographic device certification the certificate or similar document of the cryptographic device issued by the authorized professional office of the foreign power can be taken into account by the Authority.

(8) The process of certification of the cryptographic device can also be suspended simultaneously with sending of the request addressed to the foreign subject for information that is necessary for positive determination of the status of a case.

(9) During certification of the cryptographic device the Authority can determine its ability to protect tactical information.

(10) S. 48 par. 6 shall apply for the time limits laid down for issuance of the decision.

Section 50

95. **Request for cryptographic site certification and validity of the cryptographic site certificate**

(7) Cryptographic site certification shall be requested in writing with the Authority by the State body or by the facility that should operate the cryptographic site. If the facility requests cryptographic site certification, it shall be the holder of a valid FSC.

(8) The subject that requested the cryptographic site certification according to paragraph 1 shall submit documents necessary for carrying out the certification during the process of certification at the request of the Authority.

(9) The validity period of the cryptographic site certificate shall be determined by the Authority for the period not exceeding 3 years.

96.

(10) Validity of the cryptographic site certificate shall terminate

a) upon expiry of its validity period;
b) upon termination of validity of the FSC;
c) upon dissolution of the State body; or
d) by decision of the Authority on termination of the certificate validity if the cryptographic site ceased to be serviceable to perform assigned activities.

(11) Where the cryptographic site is also to be used immediately on the expiry of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide the certification of the cryptographic site. Repeated requests shall be forwarded to the Authority at least 6 months before the expiration of a validity period of the original cryptographic site certificate.

(12) The Authority shall take a decision on cryptographic site certification within 6 months of the initiation of the certification process, in very complex cases within 1 year; if the case cannot be decided within this period, with respect to its nature, the director of the Authority may reasonably extend the period, but not by more than 3 months.

Section 51

97. **Request for shielded chamber certification and validity of the shielded chamber certificate**

(1) Shielded chamber certification shall be requested in writing with the Authority by the State body or by the facility that uses the shielded chamber.

(2) The subject that requested the shielded chamber certification according to paragraph 1 shall submit documents necessary for carrying out the certification during the process of certification, at the request of the Authority.

98.

(3) Validity period of the shielded chamber certificate shall be determined by the Authority for the period not exceeding 5 years.

(4) Validity of the shielded chamber certificate shall terminate

a) upon expiry of its validity period;
b) upon termination of validity of the FSC;
c) upon dissolution of the State body; or
d) by decision of the Authority on termination of the certificate validity if the shielded chamber ceased to be serviceable for protection of classified information.

(5) Where the shielded chamber is also to be used immediately on the expiry of the validity period of its certificate, the requesting subject according to paragraph 1 shall request the Authority to provide certification of the shielded chamber. Repeated requests shall be forwarded to the Authority at least 12 months before the expiration of a validity period of the original shielded chamber certificate.

99.

(6) S. 50 par. 6 shall apply for the time limits laid down for issuance of the decision.

Section 52

100. **Contract for providing services**

101.

(1) A contract for providing services (hereinafter "the Contract") mentioned in S. 39 par. 3, S. 45 par. 4 and S. 46 par. 15 will be concluded for a fixed term or for indefinite period of time. The Contract shall be drawn up in writing. A declaration of will of contracting parties must be on the same document.

(2) The Contract can be concluded with the State body or with the facility upon their written request only on condition that the activities that are the subject matter of a Contract

102.

a) will be carried out by professionally qualified state or facility employees;
b) will be provided on the part of the State body or facility organizationally, technically and materially.

(3) The Contract with the facility can be concluded only if the facility
103.

a) is located or incorporated on the territory of the Czech Republic;
b) is a holder of the valid FSC for the appropriate security classification level; this condition does not apply if the Contract should be concluded for issuing Evaluations as outlined in S. 46 par. 15.

(4) The Contract shall contain
104.

a) identification of contracting parties;
b) specification of the subject matter of a Contract and of its scope;
c) rights and obligations of contracting parties;
d) method of control conducted by the Authority according to paragraph 6;
e) method and conditions of withdrawal from the Contract by contracting parties;
f) consent to publication of technical means on web sites of the Authority in case of Contracts for issuing Evaluations as outlined in S. 46 par. 15.

(5) Conditions according to paragraph 4 e) shall also include the stipulation that the Authority will withdraw from the Contract if the other contracting party breaches a duty provided for in this Act, implementing legal regulations or in the Contract concluded.

(6) The Authority shall verify whether the other contracting party complies with the terms of the Contract, implementing legal regulations and the contract concluded.

(7) The content of the Contract may be changed only by written agreement of contracting parties.

(8) The Contract may be terminated only in writing.

(9) In other cases provisions of the Commercial Code will be adequately applied, unless otherwise provided herein.

Section 53

105. **Delegating provisions**
106.

107. Implementing legal regulation shall stipulate

a) elements of the request for technical means certification, Information System certification, cryptographic device certification, cryptographic site certification and shielded chamber certification;
b) elements of the repeated request for Information System certification, cryptographic device certification, cryptographic site certification and shielded chamber certification;

c) documents necessary for conducting technical means certification, Information System certification, cryptographic device certification, cryptographic site certification and shielded chamber certification;
d) formats of technical means certificate, Information System certificate, cryptographic device certificate, cryptographic site certificate and shielded chamber certificate;
e) rules for determining the validity period of the technical means certificate;
f) rules and method of application of technical means upon the expiry of the validity period of its certificate;
g) method and conditions for conducting Information System certification, cryptographic device certification, cryptographic site certification and shielded chamber certification and its repetition;
h) content of the certification report according to S. 46 par. 13;
i) elements of the request for verification of electrical and electronic devices capability, security area capability or premises capability to protect classified information from its leakage by compromising electromagnetic emissions, as well as method of evaluation of their capability (serviceability); and
j) elements of request of the State body or facility for conclusion of a Contract according to S. 52.

CHAPTER X

108.

109. **Personnel security clearance, facility security clearance, special access and release from the obligation to maintain confidentiality**

Personnel security clearance and Facility security clearance

Section 54

(1) The Personnel security clearance and Facility security clearance shall be the legal instruments.

(2) The PSC shall contain

a) name, surname, maiden name;
b) day, month, year of birth, birthplace;
c) birth registration number (personal identity number);
d) nationality;
e) the highest security classification level of classified information to which the PSC gives access;
f) date of issuance and validity period;
g) official stamp and signature of the authorized representative of the Authority or, if this security clearance was issued in the electronic form, recognized electronic signature of the authorized representative of the Authority in accordance with the special legal regulation.

(3) The FSC shall contain

110.

a) identification of the facility by Firm or name, by identification number and location in case of a legal person, in case of a natural person data according to paragraph 2 a) to d);
b) highest security classification level of classified information to which the FSC gives access;
c) form of access according to S. 20;
d) date of issuance and validity period;
e) official stamp and signature of the authorized representative of the Authority or, if this security clearance was issued in the electronic form, recognized electronic signature of the authorized representative of the Authority in accordance with the special legal regulation.

Section 55

111. Period of validity of the PSC and the FSC shall be as follows
112.

a) TOP SECRET 5 years;
b) SECRET 7 years;
c) CONFIDENTIAL 9 years.

Section 56

(1) Validity of the PSC or the FSC shall terminate

a) upon expiry of its validity period;
b) on the date of enforcement of decision of the Authority (S. 123 par. 3, S. 126 par. 4) to terminate its validity (S. 101);
c) upon death of natural person or upon declaration the natural person death;
d) upon dissolution, cessation of existence of the facility;
e) upon notification of its loss or theft;
f) as a result of the damage to the extent resulting in illegibility of records in the document or causing the breach of its completness;
g) as a result of a change to data contained therein; or
h) by formation of the service relationship of the member of the Intelligence Service or labour-law relationship of the employee of the Intelligence Service assigned to the Intelligence Service, in case of PSC issued by the Authority.
i) by the end of the service relationship of the member of the Intelligence Service or labour-law relationship of the employee assigned to the Intelligence Service, or on the date when the natural person ceased to be the person outlined in S. 141 par. 1, in case of PSC issued by competent Intelligence Service or by the Ministry of the Interior;
j) by return by its holder to issuing subject;
k) from the date of delivery of the new PSC;
l) from the date of delivery of the new FSC for the same form of access of the facility to classified information;
m) from the date of delivery of decision of non-issuance of the PSC for the same security classification level; or
n) from the date of delivery of decision of non-issuance of the FSC for the same

form of access of the facility to classified information.

(2) When the validity of the FSC ends according to paragraph 1 a), b), d), j) or n), the facility shall forward the provided classified information to the providing body or to the body having the jurisdiction over classified information; if this practice cannot be complied with, it shall forward this classified information to the Authority. Classified information originated by the facility shall be forwarded by the facility to the State body having the jurisdiction over classified information, if there is no such State body, it shall be forwarded to the Authority. Classified information shall be transfered and forwarded by the facility according to this paragraph immediately after termination of validity of the FSC.

(3) When the validity of the PSC ends according to paragraph 1 a), b), j) or m), the responsible person or an individual who conducted the briefing shall prevent the natural person concerned from having access to classified information.When the validity of the PSC ends according to par. 1 j) and m) the Authority shall notify in writting his/her responsible person of termination of validity of the PSC; the Authority shall proceed in a similar way also in case of termination of the PSC according to par. 1 k) if this is PSC issued for a lower classification level.

(4) Access of a natural person or facility to classified information will not be affected by termination of the validity of the original PSC or the FSC if the holder of PSC or FSC will ask in writing the Authority 15 days from termination of its validity according to par. 1 e), f) or g) for issuance of the new security clearance; the Authority will issue a new security clearance within 5 days from the delivery of the request that replaces the original security clearance.

Section 56a

(1) In case of termination of validity of PSC according to S. 56 par. 1 h) the natural person concerned will be issued with the new security clearance by the competent Intelligence Service, which replaces the original security clearance, on the date of formation of his/her service or labour-law relationship.

(2) In case of termination of validity of PSC according to S. 56 par. 1 i) the natural person concerned will be issued with the new security clearance, which replaces the original security clearance by

a) competent Intelligence Service on the date of formation of service relationship of the member of the Intelligence Service concerning this natural person or labour-law relationship of the employee assigned to the Intelligence Service;
b) the Ministry of the Interior on the date when this natural person has become the person as outlined in S. 141 par. 1; or
c) the Authority in other cases on the date subsequent to the date of termination of validity of the original secrity clearance. The new PSC will be issued by the Authority on written request of this natural person, within 5 days from the delivery of the request. Request for the issuance of the new PSC can be made within 30 days from the date of termination of the original security clearance; the confirmation of competent Intelligence Service or Ministry of the Interior according to paragraph 3 shall be enclosed to the request.

(3) When the procedure laid down in paragraph 2 c) will be followed, the competent Intelligence Service or the Ministry of the Interior shall confirm the termination of validity of the PSC upon request of the natural person concerned within 5 days from the delivery of the request. Identification of the State body that had issued the original PSC, data listed in S. 54 par. 2 bullets a) – f) and the date of termination of the validity of this security clearance shall be laid out in the confirmation.

(4) The state body that has issued the new PSC shall request in writting the security file of the person concerned from the State body that had issued the original security clearance; the security file shall be provided within 5 days from the date of delivery of this regest.

Section 57

113. Personnel security clearance for foreign power and facility security clearance for foreign power

(1) If the natural person or facility shall have access to classified information of the foreign power he/she shall fulfil conditions according to S. 11 or S. 15 b) and, if this will be required by the foreign power, he/she shall also be the holder of the security clearance for the foreign power.

(2) If this is in accordance with security and economical interests of the Czech Republic and with obligations arising out of international agreement for the Czech Republic and if no procedure is under way focused on the person concerned according to S. 101 par. 1, the Authority will issue upon the reasonable written request of the holder of valid PSC or valid FSC

a) personnel security clearance for a foreign power; or
b) facility security clearance for a foreign power.

(3) The security clearance according to paragraph 2 shall be the legal instrument.

(4) The security clearance according to paragraph 2 contains elements as outlined in S. 54 and the marking of the highest security classification level of classified information to which this security clearance gives access shall also bear abbreviation as described in S. 21 par. 2.

(5) The security clearance according to paragraph 2 certifies that its holder has been security cleared according to Part four and that he/she is a holder of the valid PSC or FSC of the given security classification level; it certifies as well, in case of FSC, forms of access of the facility to classified information according to S. 20.

(6) The security clearance according to paragraph 2 shall be issued only for the necessary period of time which may in no case exceed the period for which the PSC or the FSC has been issued.

(7) Validity of the security clearance according to paragraph 2 will terminate

a) upon termination of validity of the PSC or FSC if this not the case of termination according to S. 56 par. 1 e) or f); or
b) for reasons determined in S. 56 par. 1 a), e) f), j), m) or n).

114.

(8) The holder of the security clearance according to paragraph 2 shall hand it over to the Authority within 15 days if

a) the validity of PSC or FSC was terminated in accordance with S. 56 par. 1 b), d) or g) to n); or
b) its validity was terminated for reasons determined in S. 56 par. 1 f)

(9) On the basis of reasonable written request of the legal person, which is not the facility, the Authority will issue time constrained confirmation of the scope of protection of classified information secured according to S. 5 by the legal person, if this is the requirement of its foreign partner or foreign power. Prior to granting confirmation the Authority shall verify to the necassary extent whether conditions of this Act have been fulfilled.

Section 58

115. **Special access to classified information**

116.

(1) The following persons may have access to classified information, irrespective of the classification of the information, without the valid PSC and briefing

a) President of the Czech Republic;
b) Deputies and Senators of the Parliament;
c) Members of the Government;
d) Ombudsman and Deputy Ombudsman;
e) judges; and
f) president, vice-president and members of Supreme Audit Office.

(2) Persons listed in paragraph 1 shall have access to classified information as from the date of election or appointment to an office for a period of its holding and to the extent necessary for its execution.

(3) Access to classified information without valid PSC may be granted to a natural person acting on behalf of the Intelligence Service, to an informant or to a natural person who has been afforded special protection according to the special legal regulation, or to the member of the Intelligence Service, who is assigned to the special reserve. The briefing of this person shall be conducted by the subject that granted access to classified information. No access to classified information of the foreign power my be granted to this person.

(4) The special legal regulation stipulates which natural persons and under what conditions may have access to classified information without valid PSC during criminal proceedings, civil legal proceedings, legal administrative proceedings and judicial administrative proceedings to the extent necessary to claim their rights and to fulfil duties within the frame of these proceedings. In these cases access to classified information may be granted only after a briefing conducted according to paragraph 5.

(5) The briefing according to S. 2 i) of persons listed in paragraph 4 shall be conducted by the individual determined by the special legal regulation. The briefing shall be conducted reasonably as outlined in S. 9 par. 1; further the briefing shall contain the file marking of the case that is the subject-matter of the proceedings, as well as instruction that the data concerning persons having access to classified information according to paragraph 4 are recorded by the Authority and can be used as described herein.

(6) With the exception of President of the Czech Republic, the President of the Senate of the Czech Republic, the Speaker of the Chamber of Deputies of the Czech Republic, Prime Minister, Minister of Foreign Affairs the persons outlined in paragraphs 1 and 4 do not have access to classifed information of the foreign power.

Section 59

117. **One-time access to classified information**
118.

(1) Upon written request of the responsible person the Authority may exceptionally and in justified cases issue its consent to access on a one-time basis to classified information classified one level higher than that to which the valid PSC or FSC has been issued, for the necessary period of time not exceeding 6 months.

(2) Consent according to paragraph 1 may be granted to the facility only for access to classified information according to S. 20 par. 1 b).

(3) Consent to one-time access according to paragraph 1 for members of Intelligence Services can be given by the director of the Intelligence Service in question, and for the Police members according to S. 141 par. 1 by the Minister of the Interior, upon written request of the competent service officer.

(4) Request according to paragraph 1 shall contain

a) justification of one-time access;
b) identification of field of classified information to which one-time access should be granted;
c) copy of the PSC or the FSC;
d) required time period of one-time access; and
e) in case of facility, written approval of the provider of classified information to give consent according to paragraph 1.

(5) The Authority shall issue consent according to paragraph 1 without delay no later than 5 days after the delivery date of the request. The responsible person or the person authorized by the responsible person who after the consent of the Authority allows access of the natural person to classified information according to paragraph 1 or 3 shall conduct a briefing of that person.

(6) No legal claim can be laid to the granting of consent to one-time access to classified information and it can be granted only once to the same person.

(7) One-time access to classified information of the foreign power may be allowed only in accordance with requirements of this foreign power.

Section 60

(8) In case of participation of the Czech Republic in an international armed conflict or in international rescue or humanitarian missions, in case of a declaration of belligerency and in case of a state of danger, emergency or state of endangering of the State, access may be granted to the natural person who is not a holder of a PSC or has not access to classified information at the security classification level RESTRICTED, or to the facility that is not a holder of a FSC or has not access to classified information at the level RESTRICTED.

(9) Access of the natural person according to paragraph 1 may be granted only if his/her trustworthiness and ability to keep confidentiality of information are undisputed.

(10) In case of access according to paragraph 1 the responsible person shall arrange a briefing of the natural person. If there is a danger of delay or by reason of other types of urgency and importance of specific task, the briefing may be replaced by a verbal familiarisation of the natural person with his/her duties in the area of protection of classified information and with consequences of their breach.

(11) A written record shall be made by the responsible person or person authorized by the responsible person of access according to paragraph 1. This written record shall be immediately forwarded by the responsible person or person authorized by the responsible person together with the briefing to the Authority; if the briefing has been replaced by the verbal familiarisation according to paragraph 3, second sentence, reference shall be made of this fact in the written record. If the access according paragraph 1 was granted by the Intelligence Service, neither the written record according to the first sentence and according to the part of the second sentence after semicolon, or the briefing, will not be forwarded to the Authority, but they will be retained by the Intelligence Service in question.

(12) When facility is granted access according to paragraph 1, its responsible person shall make a written record thereof that shall be immediately forwarded to the Authority.

(5 In case of emergency access to classified information of the foreign power may be granted only in accordance with requirements of this foreign power.

Section 61

One-time access to classified information according to S. 59 and access according to S. 60 cannot be granted to classified information classified as TOP SECRET or to classified information subject to the Special Handling Regime.

Section 62

119. Access to classified information on the basis of recognition of the security authorization issued by the autority of the foreign power

(1) Access to classified information can also be granted to the briefed natural person or to the facility in cases when the Authority recognizes security authorization issued by the authority of the foreign power that has competence to protect classified information (hereinafter "the Security Authorization"). The Authority will recognize the Security Authorization if laid down by the international agreement by which the Czech Republic is bound. Further the Authority can recognize the Security Authorization when the recognition is in accordance with foreign political and security interests of the Czech Republic; no legal claim can be laid to this recognition. If the procedure is according to the third sentence the Authority can apply for the written opinion the Ministry of Foreign Affairs and Intelligence Service in question; if the requested opinion will not be with the Authority within 30 days from the date of delivery of the request concerned then the opinion is considered to be positive.

(2) Recognition according to paragraph 1 will be carried out by the Authority upon request of the natural person not pursuing business or of the facility that are holders of the Security Authorization. The request can be also made through the authority of the foreign power having in its competence the protection of classied information; in such case the time limits according to paragraph 4 shall run from the date of delivery of the request to the Authority. The request shall contain the following

a) name or names, and surname of the Security Authorization holder;
b) date and place of birth of the Security Authorization holder;
c) nationality of the Security Authorization holder;
d) in case of facility its identification by the Firm or name, identification number and location in case of a legal person, or identification by name, surname and permanent residence address in case of a natural person;
e) reason why recognition according to paragraph 1 should be applied;
f) in case of facility that is the holder of the Security Authorization appropriate to the form of access according to S. 20 par. 1 a) determination of the form of access which is required to be recognized;
g) required validity period of the recognition; and
h) signature of the Security Authorization holder or of the responsible officer of the authority of the foreign power having the competence to protect classified information and delivery address of the recognition according to paragraph 1.

(3) Official translation of the Security Authorization shall be attached to the request according to paragraph 2 or its authenticated copy; these documents will not be required if the request had been made through the authority of the foreign power having the competence to protect classified information, if this authority proves in the request or in confirmation attached to the request that the applicant is a holder of appropriate Security Authorization.

(4) Recognition according to paragraph 1, second sentence, will be sent by the Authority to the Security Authorization holder within 10 days from the date of submission of the request. Recognition according to paragraph 1, third sentence, will be sent by the Authority to the Security Authorization holder within 60 days from the date of submission of

the request; the Authority shall not affirmatively dispose of the request if the recognition would not be in accordance with foreign political or security interests of the Czech Republic and the applicant shall be notified in writing within the outlined period thereof.

(5) Recognition according to paragraph 1 shall contain the following

120.

a) data according to paragraph 2 a) to d);
b) identification of the Security Authorization issued by the authority of the foreign power;
c) marking of the highest security classification level of classified information to which the recognition according to paragraph 1 gives access;
d) in case of facility the form of access according to S. 20;
e) date of issuance and validity period;
f) official stamp and signature of the authorized representative of the Authority or, if this recognition was issued in the electronic form, the recognized electronic signature of the authorized representative of the Authority in accordance with the special legal regulation.

121.

122.

123. **Release from the obligation to maintain confidentiality**

124.

125. **Section 63**

126.

(1) In proceedings before the State body, upon request of this body, the responsible person of the State body having the subject-matter jurisdiction over classified information, may release the natural person from the obligation to maintain confidentiality (hereinafter "the Release from Confidentiality"), save as otherwise provided herein (paragraph 8 and S. 133 par. 2).

(2) In case of cessation/termination of existence of the State body without the legal successor the Release from Confidentiality may be made by the director of the Authority.

(3) For the purpose of proceedings according to paragraph 1 the Release from Confidentiality will be further made by

127.

a) President of the Republic in case of the Prime Minister, President, Vice-President and members of the Supreme Audit Office, President and deputy President of the Constitutional Court, President and deputy President of the Supreme Court, President and deputy President of the Supreme Administrative Court, Head of the Office of President of the Republic, Ombudsman, deputy Ombudsman, Governor and deputy Governors of the Czech National Bank;
b) Chamber of Deputies in case of Deputies;
c) Senate in case of Senators;
d) Speaker of the Chamber of Deputies in case of the Head of Office of the Chamber of Deputies;
e) President of the Senate in case of the Head of Office of the Senate;
f) Prime Minister in case of ministers and heads of other central administrative offices;
g) President of the Constitutional Court in case of the Constitutional Court Justice;
h) Minister of Justice in case of judges not mentioned under bullet g) above, prosecuting attorneys and assessors, and Government in case of Director of the

Security Intelligence Service, Minister of the Interior in case of Director of International Relations and Infomation Authority and Minister of Defence in case of Director of Military Intelligence.

(4) If the obligation to maintain confidentiality concerns the subject-matter discussed by the body of the Parliament, the Chamber of Deputies or Senate can make the Release from Confidentiality after obtaining the opinion of the responsible person of the State body having the subject-matter jurisdiction over classified information.

(5) Prior to the Release from Confidentiality according to paragraph 3 the responsible person of the State body having the subject-matter jurisdiction over classified information shall be asked for his/her opinion.

(6) No Release from Confidentiality will be required in case of President of the Republic.

(7) The Release from Confidentiality only applies to classified information in question to the extent as is considered necessary and only for necessary period of time. The Release from Confidentiality shall be made in writing. Security classification of classified information shall not bet affected by the Release from Confidentiality.

(8) The Release from Confidentiality may be denied in cases where it could result in extremely serious or serios detriment to the interest of the Czech Republic or where life and limb of persons could be put in jeopardy.

128. **Delegating provisions**

129.

130. **Section 64**

131.

Implementing legal regulation shall determine the following

132.

a) the PSC format and the FSC format;
b) format of request for issuance of the PSC for the foreign power and format of request for issuance of the FSC for the foreign power;
c) formats of requests for recognition of personnel Security Authorization and facility Security Authorization.

CHAPTER XI

133.

134. **Obligations in protection of classified information**

135.

136. **Section 65**

137.

138. **Common obligations**

(1) Each individual shall forward immediately any classified information found or classified information obtained contrary to this Act, or a PSC, FSC as well as a PSC for the foreign power or a FSC for the foreign power (hereinafter “the Document Found”) to the Authority, Police or to the Embassy of the Czech Republic.

(2) Each individual who had or has access to classified information shall hold it in confidence and shall not grant access to it to any unauthorized person.

(3) In performance of the state control by the Authority each individual shall fulfil instructions of the control officer in implementing urgent measures according to S. 144 par. 1.

Section 66

139. **Obligations of the natural person who has access to classified information and obligations of the natural person who is a holder of the personnel security clearance**

(1) The natural person who has access to classified information, shall

a) observe obligations in protection of classified information;
b) hand over, within 15 days, to the issuing authority of the PSC, his/her PSC, the validity of which was terminated according to paragraph S. 56 par. 1 b) and f) to i), k) or m);
c) report immediately in writing to the issuing authority of the PSC or PSC for the foreign power, loss or theft of his/her PSC or PSC for the foreign power;
d) report immediately to the Authority changes to data given in his/her application of the natural person; limitation of the scope of reports on changes together with the manner and form of their proving shall be determined by the implementing legal regulation;
e) report immediately to the person who made his/her briefing according to S. 9 par. 1 or S. 11 par. 2 breaches of obligations determined herein;
f) take part in training according to S. 67 par. 1 b).

(2) Only obligations outlined in paragraph 1 b) to d) shall apply in case of natural person who is a holder of PSC but has not access to classified information.

Section 67

140. **Obligations of the responsible person**
141.

(1) The responsible person shall

a) provide a briefing of the natural person;
b) provide at least annually training of natural persons who have access to classified information, in the area of legal regulations on the protection of classified information and keep records of these trainings;
c) provide verification whether conditions for access of the natural person to classified information at the security classification level RESTRICTED have been fulfilled;
d) approve the Information System for operation and report this fact in writing to the Authority;
e) authorise the natural person to perform the cryptographic protection;

f) report in writting to the Authority without delay that prior to issuing of the PSC or decision according to S 121 par. 2 facts are no longer significant by which the request has been justified;
g) notify in writting the Authority without delay of termination of service relationship or labour-law, member or similar relationships, where the natural person concerned has been granted access to classified information at security classification levels TOP SECRET, SECRET or CONFIDENTIAL; this is not the duty of responsible person of the Intelligence Service or of the Ministry of the Interior in cases of members of the Police according to S. 141 par. 1;
h) control the fulfilment of other obligations determined herein.

(2) The performance of duties laid on the responsible person in S. 21 par. 5, S. 23 par. 1 b), S. 59 par. 1, S. 60 par. 5, S. 63 par.1 and 4, S. 70 par. 5 and in S. 77, par. 2 shall not be delegated to another person.

Section 68

142. **Obligations of the facility that is a holder of a facility security clearance**

The facility that is a holder of the FSC shall

a) forward to the Authority the FSC within 15 days, validity of which was terminated according to S. 56 par. 1 b), f), g), l) or n);
b) report to the Authority, without delay, loss or theft of the FSC or of the FSC for the foreign power;
c) report immediately in writting to the Authority all changes to the data given according to S. 97 a), b) or p) or S. 98 c) in the facility security questionnaire and in its security documentation; limitation of the scope of reports on changes together with the manner and form of their proving shall be determined by the implementing legal regulation;
d) report in writting to the Authority every year by the day identical to the date of issuance of FSC all changes to the data given in the application of the facility according to S. 96; limitation of the scope of reports on changes and the form of their proving shall be determined by the implementing legal regulation;
e) provide protection of classified information where validity of the FSC was terminated;
f) sent to the Authority decision on approval of the transformation project of the facility according to Transformation of Companies and Cooperative Associations Act within 15 days after its receipt.

Section 68a

Duties of the facility, which made the Statement of Facility

Facility, which made the Statement of Facility shall

a) keep security documentation of the facility within the scope of S. 98 c) and d) and provide it upon request to the provider of restricted information;

b) secure protection of classified information upon termination of access to classified information;
c) send the Statement of Facility to the Authority according to S. 15a par. 3;
d) notify according to S. 15a par. 4 in writting the Authority or provider of restricted information of termination of access to this restricted information or according to S. 15a par. 6 of termination of validity of the Statement of Facility;
e) proceed in a similar way according to S. 56 par. 2 if validity of the Statement of Facility has been terminated for reasons outlined in S. 15a par. 5;
f) make and hand over without delay to the provider of restricted information or in case of S. 15a par. 3 to the Authority the new Statement of Facility if the facility necessarily needs access to classified information at the security classification level RESTRICTED even after termination of the original Statement of Facility according to S. 15a par 5 a) or f).

Section 69

143. **Obligations of the legal person and of the natural person pursuing business who have access to classified information, and obligations of the State body**

(1) A legal person and natural person pursuing business who have access to classified information, and the State body shall

a) provide protection of classified information according to this Act and according to international agreements;
b) prepare and keep a review of positions or offices that will necessarily require access to classified information, including classified information of the European Union, North Atlantic Treaty Organisation and classified information requiring Special Handling Regime, together with the security classification level, or positions or offices that must not be discharged without a Specialist Competence Certificate according to this Act (S. 39); without prejudice to provisions of special legal regulations in the field of specialist competence;
c) notify in writing without delay the Authority of any fact that could affect issuance or validity of a PSC or FSC;
d) provide conditions for marking, recording, lending, storing, transportation, other handling and discarding of classified information and classified information subject to a Special Handling Regime in accordance with implementing legal regulation;
e) perform only such an Information System that has been certified by the Authority and approved in writing that it can be put in operation;
f) suspend operation of the Information System that does not fulfil conditions set out in certification report, and provide protection of classified information involved, and inform the Authority thereof;
g) operate only such a Communication System, the security project of which has been approved by the Authority;
h) suspend operation of the Communication System that does not fulfil conditions determined in the Communication System security project, and inform the Authority thereof;
i) use only such a device for the cryptographic protection that has been certified by the Authority, and utilise the cryptographic site only for purposes, for which it

has been certified and approved for operation;

j) keep records of natural persons who have access to classified information, records of cryptographic material, records of cryptographic protection staff, records of cryptographic device operators; records of couriers of cryptographic material and records of unauthorized handling of classified information;

k) report to the Authority any breach of obligations in protection of classified information or obligation imposed by the international agreement in the area of protection of classified information and implementation of remedial and corrective measures; this obligation does not apply to the Intelligence Services in cases according to S. 140 par. 1 a) and to the Ministry of the Interior in cases according to S. 141 par. 1, with the exception of breach of protection of classified information of the North Atlantic Treaty Organization or of the European Union;

l) establish the registry of classified information being provided (S. 79) and report changes in this registry to the Authority to the extent determined by the implementing legal regulation;

m) perform check on classified information kept in the registry of classified information by the 31st December of the calendar year and notify the Authority of the result of the check until the 15th February of the next calendar year, together with the number of classified information and its classification levels; the Intelligence Services shall send the report of classified information provided by the central registry and by the registry kept by the Ministry of Foreign Affairs according to S. 78 par. 1;

n) forward any classified information released by the foreign power or by the foreign partner of the legal person or of the natural person pursuing business, to be recorded by the Authority or by the Ministry of the Foreign Affairs according to S. 79 par. 5;

o) release in cases determined by this Act classified information to the foreign power through the central registry (S. 79 par. 2);

p) ensure that the natural person will be authorized in writing to have access to classified information with the Special Handling Regime marked as "ATOMAL";

q) as the provider of restricted information send to the Authority without delay copy of the Statement of Facility according to S. 15a par. 2;

r) as the contracting autority notify the Authority without delay in writting of the following

1. the fact that it will let a public contract beyond applicability of the Public Contracts Act or that it will make a contract, which would otherwise be the Concession Agreement beyond applicability of the Concession Act, for reasons of protection of classified information; or
2. designation of qualifying conditions of the FSC for participation in tender or concession procedures and present documents authorizing to proceed as indicated in points 1 or 2; these obligations do not relate to the Intelligence Services.

s) control compliance with other obligations determined herein.

(2) The obligation set out in paragraph 1 c) does not apply to the Intelligence Services in cases according to S. 140 par. 1 a) and to the Ministry of the Interior in cases according to

S. 141 par. 1.

Section 70

Obligations in the protection of industrial property

(1) Any person who submits to the Office of Industrial Property invention application, utility design application or topography of a semiconductor product application (hereinafter "the Applicant") shall mark on the application the proposal of the security classification level, if the subject-matter of the application is considered to contain classified information. If the Applicant is the legal person, it shall state in the application the name, surname and position or office of the responsible person.

(2) The Office of Industrial Property shall submit the application according to paragraph 1 to the Authority that, upon receiving the opinion of the central administrative office having the subject-matter jurisdiction over the subject-matter of the application, confirms the proposal of the classification level, changes it or, if subject-matter of the application does not involve classified information, denies the proposal; if the subject-matter of the application falls within the subject-matter jurisdiction of no central administrative office, no opinion will be required.

(3) The Authority shall report confirmation or change of the proposal for the security classification level in accordance with paragraph 2 to the Office of Industrial Property within a period of 60 days from the date of delivery of the application to the Authority, or it will give it a notice within the same period that it denied proposal for the security classification and return the application to the Office of Industrial Property; at the same time the Authority shall state in the notification whether the Applicant meets conditions for access to classified information.

(4) The Office of Industrial Property shall mark security classification level notified according to paragraph 3 on the application and notify immediately this level to the Applicant. The Applicant shall mark this security classification level as described (S. 21 and 22) on the subject-matter of the application; if the Applicant is the natural person not pursuing business, the Office of Industrial Property will have the position of the originator. Notification according to paragraph 3 will also be forwarded immediately to the Applicant by the Office of Industrial Property.

(5) If the subject-matter of application according to paragraph 1 contains classified information and the Applicant does not meet conditions needed for access to classified information of the given security classification level, the Office of Industrial Property shall conduct his/her briefing if the Applicant is a natural person, and if the Applicant is a legal person, the responsible person of the Applicant shall be briefed; the responsible person of the Applicant shall brief all natural persons who had access to the subject-matter of application within the frame of the legal person of the Applicant or who necessarily need it; on the basis of the briefing these persons will be considered to be persons who fulfil conditions for access to classified information involved in the subject-matter of application. Provisions of S. 9 par. 1, last sentence, and S. 11 par. 2, third sentence, will apply similarly.

Section 71

Security director (security officer)

(1) The State body that creates classified information or to that classified information has been provided, and further the legal person and the natural person pursuing business, who have access to classified information, shall establish and staff the position of the security director (security officer). Position of the security director (security officer) can be carried out by the responsible person him/herself; otherwise the security director (security officer) is directly inferior in authority to the responsible person.

(2) The State body, legal person and natural person pursuing business according to paragraph 1 shall report in writing within 15 days from staffing the position of the security director (security officer) to the Authority the name, surname and birth registration number (personal identity number) of the person carrying out this function.

(3) The security director (security officer) shall approve review of positions or functions according to S. 69 1b) that will require access to classified informationand and fulfil other duties assigned to him/her in writing by the responsible person as set out herein, including liabilities set by the responsible person, except for the cases as outlined in S. 67 par. 2; lability of the responsible person stall not be affected by the appointment of the security director (security officer). Obligation to approve review of positions or functions according to S. 69 par. 1b) shall not apply to the Inteligence Services.

(4) The position of the security director (security officer) can be held only be the natural person who fulfils conditions for access to classified information of such security classification, to which he/she will have access during the course of exercising his/her office. At the facility the natural person in the function of the security director (security officer) shall be the holder of PSC giving access to classified information at least of such security classification for which the facility has been issued with the security clearance.

(5) The position of the security director (security officer) cannot be held for more State bodies or facilities simultaneously.

Section 72

148. **Personnel project**

(1) Ministries and other central administrative offices shall prepare a personnel project every year.

(2) The personnel project shall contain

149.

a) an analysis of the situation in the field of personnel security over the past year; and
b) the assumed number of natural persons who will have to be cleared in the next year according to S. 92 a) for various security classification levels.

(3) The personnel project shall be sent by ministries and other central administrative offices to the Authority annually always until the 31st July of the corresponding calendar year.

(4) The Authority shall forward personnel projects together with its opinion to the Government always until the 30th November of the corresponding calendar year for approval.

CHAPTER XII

150.

151. **Providing of classified information within the scope of international relations**

152.

153. **Section 73**

154.

Conditions for providing classified information

Classified information can be provided within the scope of international relations unless otherwise stipulated in S. 74

a) in case of classified information at security classification levels TOP SECRET, SECRET, CONFIDENTIAL upon written request of the State body, legal person or natural person pursuing business and on the basis of written permission of the Authority;
b) in case of classified information at the security classification level RESTRICTED upon written request of the State body, legal person or natural person pursuing business and on the basis of written permission of the central administration office having the subject-matter jurisdiction over classified information; if the classified information falls within subject-matter jurisdiction of no central administrative office, on the basis of the written consent of the Authority.

Section 74

155. **Conditions for the provision of classified information between the State body and a foreign power**

(1) Fulfilment of conditions according to S. 73 a) in providing classified information between the State body and a foreign power will not be required under the following circumstances

a) an international agreement in the area of protection of classified information has been concluded, by which the Czech Republic is bound;
b) providing classified information results from the obligation of membership of the Czech Republic in the European Union;
c) classified information is provided in accordance with the special legal regulation; or
d) classified information is provided between the Intelligence Service and similar service of the foreign power in the context of cooperative activities conducted in accordance with the special legal regulation.

(2) Classified information at the security classification level RESTRICTED may be provided between the State body and the foreign power without consent laid down in S. 73 b).

Section 75

Heading deleted

(1) The following shall be included in the request according to S. 73

a) identification of the foreign power or foreign partner to be issued with the classified information;
b) reasons for which the permission or approval is requested; this does not apply if classified information should be released to the foreign power by the State body.

(2) The following shall be attached to the request of the legal person or natural person pursuing business for permission or approval according to S. 73

a) the contract for providing classified information to the foreign power or foreign partner containing specification of the classified information and conditions of its protection; or
b) if this is simultaneously the case according to S. 75a the proposal of the contract for providing classified information to the foreign power (S. 77 par. 6) or to the foreign partner, involving the security instruction; this applies in a similar way also for the State body.

Section 75a

(1) The security instruction shall become a part of the contract performing of which necessarily requires access to classified information of the foreign power, specifying conditions of protection of this information and classified information that could be originated in performance of the contract.

(2) The security instruction shall be approved prior to concluding the contract

a) by the Authority if the Authority makes it a condition or in case when no agreement has been reached according to bullet b) or when classified information does not fall within the subject-matter jurisdiction of another central administrative office;
b) by another central administrative office having the jurisdiction over classified information concerned, and, if classied information falls within the jurisdiction of more central administrative offices, by one of them, upon mutual agreement. The central administrative office, which approved the security instruction shall supervise whether it is complied with, in accordance with the Act relating to the state control.

(3) The provision of paragraph 2 shall not apply to the agreement according to paragraph 1 concluded between the foreign power or foreign partner and the Intelligence Service.

(4) The content and structure of the security instruction shall be determined by the

implementing legal regulation.

Section 76

156. **Permission and consent in the process of providing classified information**

(1) Prior to the issuance of permission according to S. 73 a) the Authority shall always require the written opinion of the Ministry of Foreign Affairs and of the Intelligence Service concerned, and further of the central administrative office having the subject-matter jurisdiction over classified information, should the permission not be required by this State body; if classified information falls within the subject-matter jurisdiction of no central administrative office, no opinion will be required. If the permission is required by the State body, the legal person or natural person pursuing business the Authority shall request from them Security Authorization of its foreign partner issued by the authority of the foreign power having the jurisdiction over the protection of classified information in the country of the foreign partner.

(2) The Ministry of Foreign Affairs, the Intelligence Service concerned and the central administrative office shall forward opinion to the Authority according to paragraph 1 within a period of 30 days from the date of delivery of its request.

(3) The Authority will issue the permission (according to) S. 73 a) within a period of 60 days from the date of delivery of the request of the State body, legal person or natural person pursuing business; the Authority shall not affirmatively dispose of the request if classified information could be endangered by its provision, and the Applicant shall be notified in writing within the outlined period thereof.

(4) The central administrative office or the Authority will issue the permission according to S. 73 b) within a period of 30 days from the date of delivery of the request of the State body, legal person or natural person pursuing business; the central administrative office or the Authority shall not affirmatively dispose of the request if classified information could be endangered by its provision and the Applicant shall be notified in writing within the outlined period thereof.

(5) No legal claim can be laid to the issuance of permission and to the granting of approval according to S. 73.

(6) The Authority shall maintain review of permissions issued according to S. 73 a).

Section 77

157. **Method of providing classified information**

158.

(1) Providing classified information at security classification levels TOP SECRET, SECRET or CONFIDENTIAL in international relations shall be carried out through the registry as outlined in S. 79 par. 2, unless otherwise stipulated in paragraphs 2 to 5, in S. 78 or in international agreement.

(2) Paragraph 1 shall not apply to providing classified information between the Intelligence
159. Service and similar services of the foreign power within the frame of co-operation carried out according to the special legal regulation. The responsible person of the Intelligence Service shall be
160. the authority for deciding on releasing classified information in these cases.

(3) Paragraph 1 shall not apply to providing classified information between the Ministry of
161. Defence, Ministry of Justice, courts, prosecuting attorney's offices, Police or customs bodies and similar bodies of the foreign power, if otherwise stipulated in the international agreement by which the Czech Republic is bound, or in the special legal regulation.

(4) State bodies and the Police shall keep records of classified information provided in accordance with paragraphs 2 and 3.

(5) Provisions of paragraph 1 and S. 73 will not be applied if classified information is provided in international relations in cases according to S. 60 par. 1.

(6) Classified information of the foreign power may be provided to another foreign power or foreign partner only in accordance with requirements of that foreign power.

Section 78

162. **Method of providing classified information of the European Union within its frame and outside the Union**

(1) Providing classified information at security classification levels SECRET or CONFIDENTIAL between the Czech Republic and member states of the European Union or between the Czech Republic and bodies of the European Union relating to the mutual co-operation of member states of the European Union according to Treaty on European Union or Treaty establishing the European Community shall be carried out through a registry kept by the Ministry of Foreign Affairs according to S. 79 par. 3.

(2) The provision of paragraph 1 will not apply to providing classified information requiring a Special Handling Regime according to S. 21 par. 3.

Section 79

163. **Registries, sub-registries and control points**
164.

(1) In registries or sub-registries of classified information classified information at security classification levels TOP SECRET, SECRET or CONFIDENTIAL, which is provided within the scope of international relations, shall be deposited or transmitted and records shall be kept in the book of records of this classified information. In control points of the registry this classified information shall be recorded in auxiliary books of records and provided to the originator.

165.

(2) The Authority shall establish and keep the central registry of classified information outlined in paragraph 1 that have been directly provided to the Authority or by the Authority and of classified information that are provided through the Authority according to S. 77 par. 1 (hereinafter “the Central Registry”).

(3) A State body, legal person and natural person pursuing business shall establish and keep a registry of classified information outlined in paragraph 1, provided to them or by them (hereinafter “the Registry”); in the Registry of the Ministry of Foreign Affairs also classified information will be kept that has been provided through the Ministry according to S. 78 par. 1. Establishment of the Registry shall be approved by the Authority upon written request of the State body, legal person or natural person pursuing business; this does not apply to the Intelligence Services. Prior to granting the approval the Authority is authorized to check the particulars in the request for establishment of the Registry, or of other facts and conditions specific to the establishment of the Registry, as applicable.

(4) The State body, legal person or natural person pursuing business can establish, in order to achieve higher level of their operational suitability in utilization of the registry, sub-registries or control points as its internal subjects.

(5) If the classified information outlined in paragraph 1 has not been provided by the foreign power or foreign partner of legal person or natural person pursuing business as set out in S. 77 par. 1 or S. 78 par. 1, the State body, legal person or natural person pursuing business shall forward classified information provided to be recorded immediately after its provision in the Central Registry, or, in case of classified information according to S. 78 par. 1, in the Registry of the Ministry of Foreign Affairs.

(6) The State body, legal person or natural person pursuing business shall report to the Authority changes in the Registry to the extent determined by the implementing legal regulation.

166.

(7) The Authority shall maintain records of established registries and carry out checks on their activities.

(8) The implementing legal regulation shall determine

a) organization and activities of the Central Registry;
b) organization and activities of the Registry, sub-registry and control point;
c) elements of the report on check on classified information kept in registry according to S. 69 par. 1 m);
d) content of written request for establishment of the Registry;
e) conditions for establishment, content and method of management of the Registry; and
f) range of changes in the Registry reported to the Authority.

167. **PART THREE**

168.

169. **SECURITY ELIGIBILITY**

Section 80

Sensitive activities

(1) The sensitive activities mean activities determined by this Act (S. 88) or by the special legal regulation, misuse of which could result in damage to the interest of the Czech Republic.

(2) Sensitive activities may be performed by a natural person who is eligible in terms of security or who is a holder of valid PSC.

(3) Such a person will be eligible in terms of security who is a holder of valid certificate of security eligibility of the natural person (hereinafter "the Certificate").

Section 81

170. **Conditions for issuance of the Certificate**

(1) The Authority will issue the Certificate to the natural person who

a) has complete legal capacity;
b) is aged 18 or over;
c) has no criminal record;
d) is personally eligible; and
e) is reliable.

(2) The condition of legal capacity will be proved by a statement made by the natural person of the legal capacity. The condition of age will be proved by ID card or by travel document of the natural person. The condition that the natural person should not have any criminal record (condition of suitability) will be proved by a statement of criminal records and, in case of a foreigner, by a similar document issued by the foreigner's parent nation, as well as by the document of the country, in which the foreigner has resided for at least 6 consecutive months in the last 10 years. The documents certifying no criminal record shall apply only for 3 months. The condition of personal eligibility will be verified as outlined in S. 13 par. 2.

Section 82

171. **Suitability (Condition of no criminal record)**

172.

173. The condition for purposes of security eligibility, that the natural person should have no criminal record, will be satisfied by the natural person who has not been finally and conclusively condemned of an intentional crime, or who is regarded to be a person who had not been condemned.

Section 83

Personal eligibility

The condition of personal eligibility for purposes of security eligibility will be satisfied by the natural person who does not suffer from any disorder or troubles that could affect his/her reliability with respect to performance of sensitive activities.

Section 84

Reliability

(1) The condition of reliability will be satisfied by the natural person if no adverse circumstance becomes known concerning this person.

(2) The adverse circumstance means

a) activities of the natural person against interests of the Czech Republic; or
b) evidence of unexplained financial or property affluance with respect to duly declared income of the natural person.

(3) Also the following can be considered to be the adverse circumstance

a) stating the false information, concealment of material information for unbiased determination of facts of a case in verifying conditions for issuance of the Certificate, or not reporting the change to the data in the application according to S. 99 or in other material provided to the Authority in annex to this application;
b) sentence imposed upon a final and conclusive judgment for a committed crime;
c) behaviour, influential conduct or untrustworthiness of the natural person that could result in misuse of performance of sensitive activities;
d) contacts with a person who has been enagaged in activities against interests of the Czech Republic;
e) repeated failure to provide necessary cooperation during the security procedure according to S. 101 par. 1; or
f) conditional discontinuace of criminal prosecution for an intentional crime or conditional postponement of the motion for punishment for an intentional crime where determined probationary period has not expired yet, or approval of settlement.

(4) Adverse circumstances as outlined in paragraphs 2 and 3 shall be traced for a period of 10 years from the date of submission of the request according to S. 99 or the period shall be covered from the applicant’s fifteenth birthday to the present, whichever is shorter.

(5) In evaluating whether the circumstance outlined in paragraph 3 constitutes the adverse circumstance, the extent to which it can affect performance of sensitive activities, period of its occurrence, its extent and character, as well as conduct of the natural person concerned in the period
as outlined in paragraph 4 shall be taken into account.

Section 85

187.

188. **Certificate**

189.

(1) The Certificate shall be the legal instrument. The validity of the Certificate shall be 5 years.

(2) The Certificate shall contain

a) name, surname, maiden name;
b) day, month, year of birth, birthplace;
c) birth registration number (personal identity number);
d) nationality;
e) date of issuance and validity period; and
f) official stamp and signature of the authorized representative of the Authority or, if this Certificate was issued in the electronic form, recognized electronic signature of the authorized representative of the Authority in accordance with the special legal regulation.

(3) Validity of the Certificate shall terminate

a) upon expiry of its validity period;
b) on the date of enforcement of a decision of the Authority (S. 123 par. 3, S. 126 par. 4) to terminate its validity (S. 101);
c) upon the death of the natural person who is a holder of the Certificate or upon declaration of a natural person's death;
d) upon notice of its loss or theft;
e) as a result of the damage to the extent resulting in illegibility of records in the document or causing a breach of its completeness;
f) as a result of change to some data contained therein;
g) upon return of the Certificate by its holder to its issuing autority; or
h) on the date of delivery of PSC or of the new Certificate.

(4) The performance of sensitive activities will not be affected by termination of validity of the original Certificate if the holder of the Certificate requests the Authority over a period of at least 15 days prior to termination of its validity according to paragraph 3 d), e) and f) in writting for issuance of the new Certificate; the Authority shall issue within 5 days from the delivery of the request a new Certificate that replaces the original one.

(5) The format of the Certificate shall be determined by the implementing legal regulation.

Section 86

190. **Obligations of the legal person, natural person pursuing business and of the State body**

191. A legal person, natural person pursuing business and the State body shall

a) ensure that the sensitive activities will be performed by a natural person who is a

holder of the valid Certificate or PSC;

b) keep records of natural persons who perform sensitive activities and who are in service relationships or in labour-law relationships, member relationships or similar relationships in respect of them;
c) report in writting to the Authority without delay that prior to issuance of the Certificate or decision according to S. 121 par. 2 facts are no longer signifiant by which the request for the Certificate has been justified;
d) report in writing to the Authority any other fact than that outlined under bullet c), which could affect issuance of the Certificate or decision to terminate its validity or validity of PSC (S. 101); and
e) report in writting to the Authority without delay that the performance of sensitive activities has been initiated or that it has been terminated for reasons of termination of service relationship or labour-law relationship, member relationship or similar relationship of the holder of the Certificate or security clearance.

Section 87

Obligations of the natural person

(1) The natural person who is a holder of the Certificate shall

a) hand over the Certificate within 15 days to the Authority, the validity of which was terminated according to bullets b), e), f) or h);
b) report immediately in writing to the Authority the loss or theft of the Certificate;
c) report immediately to the Authority changes to data set out in his/her application for the Certificate; limitation of the scope of reports on changes together with the manner and form of their proving shall be determined by the implementing legal regulation.

(2) Any individual shall forward immediately the Certificate found to the Authority, to the Police or to the Embassy of the Czech Republic.

Section 88

192. **Performance of sensitive activities for the needs of the Intelligence Services**

(1) Actions of persons not mentioned under S. 140 par. 1 a) performed for the Intelligence Service upon agreement, in connection with the performance of the state administration or for other reasons, will be considered to be the sensitive activities for the needs of the Intelligence Service.

(2) Conditions of security eligibility of the natural person who should perform sensitive activities for the Intelligence Service shall be verified by the Intelligence Service.

(3) The Intelligence Service will verify conditions according to S. 81 on its own initiative to

193. the extent necessary for the performance of sensitive activities. A security clearance procedure will not be carried out and no Certificate will be issued.

(4) The Intelligence Service will allow the natural person to perform sensitive activities if conditions according to S. 81 will be satisfied by him/her for the period of time necessary to perform these activities.

194.

195. **PART FOUR**

196. **SECURITY CLEARANCE PROCEDURE**

197. **CHAPTER I**

198.

Common provisions

Section 89

199. **Common principles of the security clearance procedure**

(1) The Authority shall act during the security clearance procedure (hereinafter "the Procedure") in such a way as to ascertain without any false statement or omission facts of the case to the extent necessary for the decision.

(2) During the Procedure, personal honour and dignity must be protected of all persons involved in the Procedure.

(3) During the Procedure all negotiations shall be conducted and documents made in the Czech language, with the exception of the exercise of rights of a member of the national minority according to the special legal regulation. Documents made in a foreign language shall be presented by participant in the Procedure in original wording together with officially authenticated translation into the Czech language.

(4) The Authority shall create conditions to avoid any damage to or abridgement of rights of the participant in the Procedure for the reason of his/her health handicap.

(5) The Procedure shall be closed for the public.

(6) The participant in the Procedure may authorise a lawyer or another deputy whom he/she chooses to represent him/her in the Procedure. Authority for representation shall be proved by a letter of attorney. The participant may be represented only by one deputy. Representation shall be out of the question in case of personal acts.

(7) The participant in the Procedure and his/her representative shall have the right to inspect the security file before the issuance of the decision and to make extracts thereof, with the exception of the part of the security file (S. 124) containing classified information.

(8) Actions aimed towards the Authority can also be performed in the form of delivery to data box of the Authority or in the electronic form signed by the recognized electronic signature, if this is compatible with requirements of this Act.

Section 90

200. **Exclusion from the Procedure**

201.

(1) Any employee of the Authority directly participating in the Procedure (hereinafter "the Person in the Authority") who can be reasonably anticipated to have such interests in the course and results of the Procedure, with respect to his/her relation to the case, to the participant in the Procedure or to his/her representative, for which his/her impartiality can be in doubt, shall be excluded from all acts associated with the Procedure, during which he/she could affect the result of the Procedure.

202.

(2) Also such a Person in the Authority shall be excluded who participated in the Procedure in the same case at another stage of the Procedure.

(3) The participant in the Procedure may lodge an objection against the prejudice of the Person in the Authority within 15 days from the date on which he/she became aware of the Person in the Authority participating in the Procedure. The objection against the prejudice shall contain, among common formalities, against what Person in the Authority the objection is directed, what is considered to be a reason for doubts concerning impartiality of the Person in the Authority and by what evidence his/her allegation can be substantiated. The later submitted objection will not be taken into account.

(4) The Person in the Authority who becomes aware of circumstances indicating his/her prejudice shall immediately notify his/her superior officer thereof. Until such time as the superior officer has decided whether he/she shall be excluded, the Person in the Authority may perform only such acts that cannot be delayed.

(5) No remonstrance shall be permitted against exclusion of the Person in the Authority.

(6) Paragraphs 1 and 3 to 5 will be applied similarly also in case of participation of experts and interpreters in the Procedure.

Section 91

203. During the Procedure the Authority shall decide applications according to S. 94, 96 and 99 and termination of validity of the PSC, FSC or of the Certificate according to S. 101.

Section 92

Participant in the Procedure

204. The following subjects shall be participants in the Procedure

a) in case of the Procedure concerning applications according to S. 94 or 99 the natural person who requests for issuance of the PSC or Certificate, or person for whom the issuance of the PSC will be required according to S. 93 par. 1) b);

b) in case of the Procedure according to S. 96 the facility that requests for issuance of the FSC;
c) in case of the Procedure concerning termination of validity of the PSC, FSC or Certificate according to S. 101 the holder of these legal instruments.

205. **CHAPTER II**

206.

207. **Course of the Procedure**

208.

209. **Section 93**

210.

211. **Initiation of the Procedure**

212.

(1) The Procedure will be initiated on the date of

a) delivery of the written application to the Authority according to S. 94, 96 or 99;
b) delivery of the request of the body of the European Union to the Authority for issuance of the PSC – for a national of the Czech Republic who is an employee of a body of the European Union or of the international organization, of which the Czech Republic is the member;
c) delivery of written notice of the Authority to the holder of a PSC, FSC or Certificate of initiation of the procedure concerning termination of validity of these legal instruments (S. 101);
d) delivery of the decision of the director of the Authority on remonstrance (S. 125) issued according to S. 131 par. 3.

(2) In case of the procedure concerning termination of validity of the PSC or Certificate the Authority shall also notify the responsible person of the holder of these legal instruments of initiation of the procedure according to paragraph 1 c).

213.

214. **Application of the natural person**

215.

216. **Section 94**

217.

(1) The application for issuance of the PSC (hereinafter "the Application of the Natural Person") shall contain to the extent determined by the implementing legal regulation written justification of the need of the individual concerned to have access to classified information together with indication of security classification level, and indication of the post or function according to S. 69 par. 1 b) that shall be confirmed by the responsible person or by the body that will provide classified information to the natural person.

(2) The following shall be attached to the application according to paragraph 1 by the natural person

a) completed questionnaire of the natural person in paper and electronic forms;
b) documents confirming correctness of data stated in the questionnaire to the extent and in the form determined by the implementing legal regulation;
c) statement concerning personal eligibility;
d) statement of legal capacity;

e) one photograph sized 35 x 45 mm corresponding to the present appearance of the natural person, from the front view with the length of head from eyes to chin 13 mm as a minimum, without glasses with dark glass, with the exception of blind individuals, the person shall be dressed in civil clothes and without headgear, if its use is not substantiated by religious or health reasons; in such cases the headgear shall not cover the face in such a way that identification of the natural person would be made impossible;

f) if the natural person is a foreigner, the document similar to certificate of no criminal records of the state of which the person is the national, as well as of the state in which the person has resided for at least 6 consecutive months; this document shall cover coresponding period according to S. 14 par. 4 and shall apply only for 3 months;

g) statement of release from confidentiality of the tax administrator having subject-matter and territorial jurisdiction and of any other person participating in administration of taxes according S. 52 par. 2 of the tax rules, to the full extent of data for purposes of performing of security clearance procedure.

(3) Appendices according to paragraph 2 shall be considered to be a part of the Application of the Natural Person.

(4) When the natural person should have access to classified information also immediately on the expiry of the validity period of his/her PSC, he/she shall request in writing the Authority for issuance of the new PSC before expiration of a validity period of the current PSC at least within the following periods

a) 3 months in case of a PSC for the security classification level CONFIDENTIAL;
b) 7 months in case of a PSC for the security classification level SECRET; and
c) 10 months in case of a PSC for the security classification level TOP SECRET.

(5) Application according to paragraph 4 shall comply with elements according to paragraph 1 and appendices according to paragraph 2 shall be attached. Data in the personnel questionnaire shall be completed as described by the implementing legal regulation. Documents according to paragraph 2 b) will be attached to the application only if during the validity period of the PSC a change occurs to the data.

(6) If the natural person requests issuance of the new PSC according to paragraph 4 for the same security classification level, for which he/she has been issued with the current PSC, investigation for determining whether the new PSC can be issued shall be carried out retrospectively, covering at least the period since issuance of the previous PSC.

(7) If the body of the European Union or of the international organization of which the Czech Republic is the member requests issuance of the PSC according to S. 93 par. 1 b), the natural person concerned shall proceed in accordance with paragraphs 2 to 6 similarly.

(8) The reason laid out in the application, why the access of the natural person to classified information shall be necessary, shall continue to be valid throughout the Procedure according to S. 93 par. 1 a) b) or d).

Section 95

Personnel Questionnaire

(1) The personnel questionnaire shall contain the following items

a) name, surname including all earlier used surnames, and university degrees;
b) date, months, year and place of birth and birth registration number (personal identity number);
c) citizenship status (nationality), present and past;
d) permanent address and address of any other residence where the natural person lives or lived in the last 10 years for at least 90 consecutive days;
e) data concerning an identity card where a foreigner is in question;
f) name of employer and identification of the position being held or identification of activities being exercised;
g) names of previous employers including data of formation and termination of employment relationship or service relationship;
h) family status;
i) continuous stays abroad exceeding 90 days;
j) orders to execute judgment;
k) criminal proceedings;
l) previous security clearance procedures;
m) membership of, contacts and associations with former and present security services of a foreign power or with its services in the area of intelligence and with units outlined in S. 14 par. 3 a), except for the cases where these contacts result from employment or service obligations after the year 1990;
n) personal contacts with foreign nationals or with national of the Czech Republic living in non-EU or non-NATO countries, except for the cases where these contacts result from employment or service obligations after the year 1990 if these contacts can be assumed in a justified manner to be significant;
o) any narcotics or psychedelic drugs abuse, which are described in the law regulating the area of habit forming substances and alcohol consumption;
p) pathological gambling;
q) treatment for addiction to substances listed under bullet o) and to alcohol and treatment for pathological gambling;
r) highest level of education achieved;
s) property owned;
t) membership of associations, foundations and beneficiary associations within the most recent 5 years;
u) delivery address;
v) data according to bullets a) to d) and f) concerning spouse or partner and persons aged 18 or over sharing the natural person's living quarters.

(2) Curriculum vitae and statement of truthfulness and completeness of data listed in personnel questionnaire shall be a part of the questionnaire.

(3) Residence and stays according to paragraph 1 d) and i) and S. 94 par. 2 f) shall be considered continuous even in case of its interruption of short term duration.

218. **Application of the facility**

Section 96

(1) Application of the facility shall contain to the extent determined by the implementing legal regulation written justification of the need of the facility concerned to have access to classified information together with an indication of security classification level and the form of occurrence of classified information.

(2) The following shall be attached to the application according to paragraph 1 by the facility

a) completed questionnaire of the facility in paper and electronic forms;
b) security documentation of the facility; and
c) documents necessary to verify compliance with conditions according to S. 16 to the extent and in the form determined by the implementing legal regulation;
d) statement of release from confidentiality of the tax administrator having subject-matter and territorial jurisdiction and of any other person participating in administration of taxes according S. 52 par. 2 of the tax rules, to the full extent of data for purposes of performing of security clearance procedure.

(3) Appendices according to paragraph 2 shall be considered to be a part of the application of the facility.

(4) When the facility should have access to classified information also immediately on the expiry of the validity period of its present FSC, it shall request in writing the Authority for issuance of the new FSC before expiration of a validity period of the current FSC at least within the following periods

a) 7 months in case of a FSC for the security classification level CONFIDENTIAL;
b) 9 months in case of a FSC for the security classification level SECRET; and
c) 11 months in case of a FSC for the security classification level TOP SECRET.

(5) Application according to paragraph 4 shall comply with elements according to paragraph 1 and all appendices according to paragraph 2 shall be attached. The data in questionnaire shall be completed to the extent determined by the implementing legal regulation. Only such changes shall be completed in the security documentation of the facility that have not been reported to the Authority according to S. 68 d).
219.

Section 97

220. **Facility Questionnaire**

221. The facility questionnaire shall contain the following items:

a) valid data that are entered in the Commercial Register, Register of Trades or similar register or records, but in any case indication of birth registration number (personal identity number) if assigned, as well as of date, place, district and state of birth, even if not entered into such register or record;

b) birth registration number (personal identity number) if assigned, as well as the date, place, district and state of birth, company and identification number of members of the company if these are not data recorded in the Commercial Register;
c) names of bank institutions and numbers of valid bank accounts and information on accounts kept at consumer and credit cooperative associations;
d) immovables and non-residential premises of the facility owned and under-lease housing the security area according to S. 25 including their address;
e) data concerning conducted ordinary financial statements, if the facility keeps accounts, or data on tax returns, if the facility keeps tax records according to other legal regulation, as well as data concerning ordinary financial statements by certified auditor if stipulated so by other legal regulation, for the past 5 years;
f) loans and credits provided and accepted within the past 5 years;
g) contracts subject matter of which contains classified information;
h) foreign business partners other than that of member states of the European Union with total financial volume of trades carried out and exceeding 2 milion crowns within the past 5 years;
i) Czech business partners and business partners from member states of the European Union together with total annual payments of trades carried out and exceeding 20% of yearly turnover within the past 5 years;
j) information on submission of insolvency petition;
k) information on desicion concerning the insolvency petition;
l) information on the method of bankruptcy settlement;
m) information on termination (dissolution) of the facility;
n) performance of obligations in respect of the State according to S. 17 par. 2 a) and b);
o) data concerning the responsible person of the facility, which are the name, surname, birth registration number (personal identity number) if assigned, date of birth and position being held at the facility; and
p) criminal proceedings.

222.
223. **Section 98**

Facility security documents

224. Facility security documents shall determine the system of protection of classified information at the facility, shall be deposited with the facility, updated periodically, and contain the following

a) listing of classified information held by the facility, indicating its originator and security classification levels, and if classified information has been provided to or created by the facility upon order, also the specification of this order shall be indicated, and further the specification of classified information to which the facility should have access, indicating its originator and security classification level, and if classified information should be provided to or created by the facility upon order also the assumed specification of this order shall be indicated;
b) analysis of possible threat to classified information, suitable and effective protective measures to ensure risks reduction;

c) methods of implementation of individual modes of securing of the protection of classified information;
d) list of positions where access to classified information is anticipated and list of persons who should have access to classified information, indicating their birth registration number (personal identity number) and security classification level required by these persons in their application for issuance of PSC, and in case of the PSC already issued its number and date of issuance and security classification level for which it was issued, in case of the Notice the date of its issuance and in case of the Certificate its number and date of issuance.

Application for the Certificate

Section 99

(1) Application for the Certificate shall contain to the extent determined by the implementing legal regulation written justification of the performance of sensitive activities confirmed by the responsible person or by the person authorized by the responsible person.

(2) The following shall be enclosed in the application according to paragraph 1 by the natural person

a) completed questionnaire in paper and electronic forms;
b) statement of personal eligibility;
c) documents certifying the correctness of data stated in the questionnaire to the extent and in the form determined by the implementing legal regulation;
d) statement of release from confidentiality of the tax administrator having subject-matter and territorial jurisdiction and of any other person participating in administration of taxes according S. 52 par. 2 of the tax rules, to the full extent of data for purposes of performing of security clearance procedure;
e) statement of legal capacity;
f) if the natural person is a foreigner, the document similar to certificate of no criminal records of the state of which the person is the national, as well as of states in which the person has resided for at least 6 consecutive months within a period covering the last 10 years and this document shall apply only for 3 months; and
g) one photograph sized 35 x 45 mm corresponding to the present appearance of the natural person, from the front view with length of head from eyes to chin 13 mm as a minimum, without glasses with dark glass, with the exception of blind individuals, the person shall be dressed in civil clothes and without headgear, if its use is not substantiated by religious or health reasons; in such cases the headgear shall not cover the face in such a way that identification of the natural person would be made impossible.

(3) Appendices according to paragraph 2 shall be considered to be a part of the application for the Certificate.

(4) If the natural person should perform sensitive activities also immediately on the expiry of the validity period of the Certificate, he/she shall request the Authority for issuance of the new Certificate at least 5 months before the expiration of the validity period of the

current Certificate.

(5) Application according to paragraph 4 shall comply with elements according to paragraph 1 and appendices according to paragraph 2 shall be attached. Data in the questionnaire shall be completed as described by implementing legal regulation. Documents according to paragraph 2 c) will be attached to the application only if during the validity period of the Certificate a change occurs to the data that are contained in these documents.

(6) If a natural person requests issuance of a new Certificate according to paragraph 4, investigation of conditions for determining whether the new Certificate can be issued shall be carried out retrospectively, covering at least the period since the issuance of the current Certificate.

(7) For purposes of proving suitability the Authority shall request a copy of criminal conviction records according to special legal regulation. The request for issuance of a copy of criminal conviction records and a copy of criminal conviction records shall be provided in electronic form in a manner making the remote access possible.

(8) The reason for performance of sensitive activities laid out in the application for the Certificate shall continue to be valid throughout the Procedure according to S. 93 par. 1 a) b) or d).

Section 100

225. **Questionnaire**

The questionnaire according to S. 99 par. 2 a) shall contain items determined in S. 95 par. 1 a) to u) and in S. 95 par. 2.

Termination of validity of Personnel Security Clearance, **Facility Security Clearance or Certificate**

Section 101

226.

(1) The procedure concerning termination of the PSC, FSC or Certificate shall be initiated by the Authority if there is a reasonable doubt whether the holder of such legal instrument continues to meet conditions for its issuance (S. 12, 16 and 81).

(2) If the holder of the PSC, FSC or of the Certificate no longer meets conditions for issuance of such legal instrument, the Authority will terminate its validity.

(3) The procedure concerning termination of the PSC, FSC or Certificate can neither be suspended according to S. 112 nor terminated according to S. 113 except termination of the procedure according to S. 113 par. 1 i) or j).

227. **Common provisions**
228.

229. **Section 102**
230.

(1) If the Application of the Natural Person, application for Certificate or application of the
231. facility has not complied with required elements, the Authority will afford assistance to the participant in the procedure in elimination of these formal defects. If these defects cannot be eliminated on the spot, the Authority shall request the participant in the Procedure without delay to eliminate these defects within 30 days of the service of the request; briefing on consequences shall be part of the request, if the data necessary for continuing the Procedure will not be completed in time [S. 113 par. 1 c)].

(2) The Authority will acknowledge acceptance of the application of a natural person, application for the Certificate or application of the facility, at the request of the participant in the Procedure.

232.
233. **Section 103**
234.

(1) If necessary for complete and exact finding of actual facts of a case, the Authority is entitled to request from the participant in the Procedure specification of data listed in the application according to S. 94, 96 and 99 and giving notice of additional data to verify fulfilment of conditions for issuance PSC, FSC or Certificate. For this purpose the Authority will request in writing the participant in the Procedure to submit this specification to the Authority within 14 days and in case of application submitted according to S. 96 within 30 days of the service of the request.

(2) During the Procedure the participant in the Procedure shall notify without delay in writing the Authority of any changes to the data listed in the application according to S. 94, 96 and 99; limitation of the scope of reports on changes together with the manner and form of their proving shall be determined by the implementing legal regulation.

235. **Section 104**
236.
237. **Witness**
238.

(1) Any individual shall testify as a witness for the purpose of finding the facts of a case and determination of possible security risks, and attend on summons at the Authority. It must be clear from the summons, when, where and in what case the witness shall attend and what are the consequences in law arising from the fact of non-attendance (S.115, S.116). The witness shall testify truthfully and completely. Any individual shall not be examined as a witness, who would breach the protection of classified information or the duty to maintain confidentiality imposed or recognized by the law, unless he/she has been released from this duty. The witness can refuse to give the testimony only if it could put him/her or an immediate family member at risk of criminal prosecution. The testimony may also be refused by the person who has close ties of affection to a participant in the Procedure.

(2) Prior questioning the Authority shall establish the identity of a witness and brief

him/her according to paragraph 1 and on the legal consequences of untrue or incomplete testimony (S. 116).

(3) A report on witness testimony shall be made. S. 105 par. 5 and 6 shall apply by analogy concerning making the report on a witness testimony.

(4) The witness can also be required to provide written statement to facts given to him by the Authority. Signature of the witness shall be on each page of the document containing his/her statement. Concerning other stages paragraphs 1,5 and 6 will be used.

(5) The Authority shall reimburse proved cash expenses to the witness according to the law regulating travel allowances and loss of earnings. A claim shall be filed within 5 days from the witness testimony, otherwise it will expire. The witness shall be warned in advance thereof.

(6) Any Police officer or member of the Intelligence Service shall not be examined as a witness, who participates in the Procedure.

239.

(7) Acts in the Procedure according to S. 107 to 109 shall not be replaced by the witness testimony.

Section 105

Security interview

(1) When information comes to light during the Procedure that shall be inquired in order to find the actual facts of the case, the security interview shall be conducted with the participant in the Procedure by the Authority; in case of a participant in the Procedure who requests a PSC for the security classification level TOP SECRET the security interview by the Authority shall be conducted in all cases.

(2) The participant in the Procedure shall be summoned to the security interview in writing. It must be clear from the summons, when, where and in what case and for what reason the participant in the Procedure shall attend and what are the consequences in law arising from the fact of non-attendance [S. 113 par. 1 d)].

(3) During the course of a security interview the participant in the Procedure shall represent facts truthfully and completely personally; no lawyer or representative of the participant in the Procedure is entitled to intervene in the course of the interview.

(4) Prior to commencement of the security interview each participant in the Procedure shall be briefed in writing on the importance and purpose of the interview and on possible consequences in case of false or incomplete statement [(S. 113 par. 1 h)].

(5) A report on the security interview shall be made. The report shall contain the place, time and subject matter of the interview, as well as data permitting identification of the participant in the

240. Procedure, Person in the Authority and of other individuals participating in the interview.

(6) The report shall be signed by the participant in the Procedure, Person in the Authority or recorder or interpreter, as applicable; signature of the participant in the Procedure shall be on each page of the record. Refusal to sign the record and reasons for this refusal shall be entered in the record. Upon request of the participant in the Procedure the Person in the Authority will issue copy of the record. The security interview may be recorded on audio or video media only with consent of the participant in the Procedure; the record shall be made whenever requested by the participant in the Procedure. This record shall be the part of the security file (S. 124).

(7) No classified information shall be disclosed during the course of a security interview.

(8) A security interview with a participant in the Procedure with long-term residence abroad may be substituted by his/her written statement. All information shall be communicated by the Authority to this individual that should be the subject of the statement. The signature of the participant in the Procedure shall be on each page of the written statement.

Section 106

Expert

(1) If during investigation of condition of personal eligibility in cases according to S. 13 and 83 facts are revealed by the Person in the Authority giving rise to doubts as to the personal eligibility of the participant in the Procedure, the Authority will appoint an expert for making an expert's report on personal eligibility.

(2) If the expert's report is needed for expert evaluation of facts important for the final decision and if these facts are not as outlined in paragraph 1, the Authority will appoint the expert.

241.

(3) The costs of making an expert's report according to paragraph 1 and 2 will be reimbursed by the Authority.

Acts during the course of the Procedure

Section 107

242. **Acts during the course of Procedure for granting the personnel security clearance**

(1) During the course of the Procedure for granting the PSC for the security classification level CONFIDENTIAL the Authority will require the necessary information from the competent State body, legal person or natural person pursuing business, provided they handle such information, for verification of conditions for issuance of this security clearance.

(2) During the course of the Procedure for granting the PSC for the security

classification level SECRET, the Authority shall proceed in accordance with paragraph 1, and further verify the identity of the participant in the Procedure; concerning verification of identity of the participant in the Procedure it may contact the Intelligence Service concerned or the Police, as necessary. If information obtained is not sufficient for full determination of facts of the case, these can be verified or completed upon the request of the Authority by investigation of the Intelligence Service concerned or the Police with respect to the participant in the Procedure and with respect to individuals aged 18 or over living in a common household with the participant in the Procedure.

(3) During the course of the Procedure for granting the PSC for the security classification level TOP SECRET, the Authority shall proceed in accordance with paragraph 2, and further ask the Intelligence Service concerned for investigation aimed at occurence of security risks in the background of the participant in the Procedure.

(4) The Intelligence Services and the Police shall comply with the request of the Authority

243. according to paragraphs 2 and 3 and submit to the Authority report on results of investigations being requested.

(5) If information obtained during the course of the Procedure for granting the PSC for the security classification level CONFIDENTIAL is not sufficient for full determination of facts of the case, the Authority shall be entitled to verify it by acts according to paragraphs 2 and 3, and during the course of the Procedure for granting the PSC for the security classification level SECRET according to paragraph 3. In these cases the Authority shall request written consent of the participant in the Procedure and brief him/her at the same time on legal consequences if the Authority does not receive the written consent [S. 113 par. 1 e)].

(6) If the Procedure is conducted upon application according to S. 94 par. 4, the Authority shall be entitled to perform acts according to paragraphs 1 to 5. Provisions of the paragraph 5 of the second sentence shall apply by analogy.

244.

245.

246. **Section 108**

247.

248. **Acts during the course of the Procedure for granting the facility security clearance**

249.

(1) During the course of the Procedure for granting the FSC for the security classification level CONFIDENTIAL, the Authority will require the necessary information from the competent State body, legal person or natural person pursuing business, provided they handle such information, in order to determine the economic stability, security eligibility and to verify ownership relations of the facility and its ability to secure the protection of classified information.

250.

(2) During the course of the Procedure for granting the FSC for the security classification level SECRET, the Authority shall proceed in accordance with paragraph 1, and undertake further actions to verify commercial relations of the facility.

(3) During the course of the Procedure for granting the FSC for the security classification level TOP SECRET, the Authority shall proceed in accordance with paragraph 2, and undertake further actions to verify important capital and finacial relations of the

facility.

(4) Persons in the Authority shall be authorized to enter premises, units, institutions, facilities, plants or other areas and land of the facility with a view to verifying conditions of granting the FSC and require submission of necessary documents by the facility.

(5) If the Authority cannot verify relations outlined in paragraphs 1 to 3 or other facts to ascertain possible security risk at the facility or its capability to secure the protection of classified information the Authority can ask the competent Intelligence Service or the Police for this verification.

(6) The Intelligence Services and the Police shall comply with the request of the Authority according to paragraph 5 and submit to the Authority a report on the results of investigations being requested.

(7) If the information obtained by acts according to paragraph 1 or 2 during the course of the Procedure for granting the FSC for corresponding classification level is not sufficient for full determination of facts of the case, the Authority shall be entitled to verify it by acts according to paragraphs 2 or 3 for the Procedure relating to the higher security classification level. In these cases the Authority shall request written consent of the participant in the Procedure and brief him/her at the same time on the legal consequences if the Authority does not receive the written consent [S. 113 par. 1 e)].

(8) If the Procedure is conducted upon application according to S. 96 par. 4, provisions of paragraphs 1 to 7 shall apply by analogy.

Section 109

251.

252. **Acts during the course of Procedure for granting the Certificate**

253.

(1) During the course of Procedure for granting the Certificate the Authority will require the

254. necessary information from the competent State body, legal person or natural person pursuing business, provided they handle such information.

(2) If the information obtained according to paragraph 1 is not sufficient for full determination of facts of the case, it can be verified or completed by other necessary acts according to S. 107, appropriate to the purpose of the Procedure; in these cases the Authority shall request written consent of the participant in the Procedure and brief him on legal consequences if the Authority doeas not receive the written consent [S. 113 par. 1 e)].

(3) If the Procedure is conducted upon application according to S. 99 par. 4, the Authority shall be entitled to perform acts according to paragraphs 1 and 2. Provisions of the paragraph 2 of the part of the sentence after the semicolon shall apply by analogy.

Section 110

(1) Within the period of validity of the PSC, Certificate or FSC, prior to issuance of

the PSC for a foreign power or of the FSC for a foreign power according to S. 57, the Authority shall verify by acts of the Procedure whether the natural person or facility continue to satisfy conditions for issuance of the PSC, Certificate or FSC.

(2) Upon request of the security authority of the member state of the North Atlantic Treaty
255. Organization, European Union or another state, with which the Czech Republic has concluded the international agreement, having jurisdiction over the protection of classified information, the Authority shall perform acts of the Procedure concerning a person who is being security cleared in the state concerned for access to classified information.
256.
257.
258. **Section 111**
259.

260. In performing acts according to S. 107 and 108, S. 109 par. 1 and S. 110 the Authority is entitled to provide to the State body, legal person or to the natural person pursuing business to the extent necessary the requisite personal data relating to the information being requested.
261.
262.
263. **Section 112**
264.
265. **Suspension of the Procedure**

(1) The Authority shall suspend the Procedure by its decision if

a) another procedure takes place relating to the question significant for issuance of a decision according to this Act;
b) the participant in the Procedure has been invited by the Authority to remove shortcomings of the natural person application, facility application, Certificate application or of the remonstrance, or to supplement other data required by the Authority, or if the participant in the Procedure has been summoned to interview;
c) the participant in the Procedure represented by more responsible persons, but not in conformity, has been invited by the Authority to reach conformity within a prescribed period, or to delegate the negotiation of the subject matter on only one responsible person;
d) the witness cannot be examined whose statement is important for determination of actual facts of the case;
e) the participant in the Procedure asks for suspension by reason of long-term impediment to participation in the Procedure, but for no longer than 60 days; or
f) the expert has been appointed to make the expert's report.

(2) The Procedure shall be suspended on the date of delivery of decision on suspension of the Procedure to postal services licence holder or to the special postal licence holder, on the date of personal receipt of such decision by the participant in the Procedure, if the Authority provides such delivery, or by delivery to data box of the participant in the Procedure.

(3) No remonstrance shall lie against the decision to suspend the Procedure.

(4) The Authority shall proceed with the Procedure as soon as obstacles of its suspension ceased to exist or the time limit set out in paragraph 1 e) expired. The participant in the Procedure shall be notified in writing by the Authority thereof.

(5) During suspension of the Procedure the time limits according to S. 117 and S. 131 par. 6 do not run.

Section 113

Termination of the Procedure

(1) The Authority shall terminate the Procedure by its decision if

a) the participant in the Procedure withdraws the natural person application, facility application, Certificate application or remonstrance (S. 125);
b) the participant in the Procedure does not fulfil conditions laid down in S. 6 par. 2 or S. 81 par. 1 a), b) or c);
c) the participant in the Procedure has not removed shortcomings within a prescribed period in the natural person application, facility application, Certificate application or remonstrance (S. 125);
d) the participant in the Procedure did not repeatedly attend the interview without excuse containing substantial reasons;
e) the participant in the Procedure did not give his consent according to S. 107 par. 5, S. 108 par. 7 or S. 109 par. 2;
f) the participant in the Procedure has not reached conformity in negotiations of responsible persons within a prescribed period of time or has not delegated only one responsible person to the negotiation;
g) complete and correct facts of the case cannot be determined because the participant in the Procedure lives or has lived in a foreign country over a long period of time;
h) the participant in the Procedure has submitted false or incomplete statement or does not cooperate in any other way as necessary and the case cannot be decided on the basis of the given facts of the case;
i) the participant in the Procedure died or has been declared dead or it was dissolved, or due to its termination; or
j) in the Procedure according to S. 101 its reason or subject have disappeared.

(2) The Intelligence Services and the Ministry of the Interior shall also terminate the Procedure by decision if the reason of the Procedure according to S. 140 par. 1 a) and S. 141 par. 1 disappears by virtue of incompetence of these State bodies and the Application of the Natural Person has not been withdrawn.

(3) The Authority may not to proceed with the security clearance procedure concerning issuance of the PSC or Certificate on notice of the responsible person according to S. 67 par, 1 f) or S. 86 c).

(4) The provision of paragraph 1 j) will not apply for termination of remonstrance proceedings (S. 131 par. 1) brought against the decision to terminate validity of the PSC, FSC or Certificate.

(5) No remonstrance shall be permitted against the decision to terminate the Procedure according to paragraph 1 a), b), e), f), g), i) and j) and according to paragraph 2.

Securing of the purpose and course of the Procedure

Section 114

Summons

(1) The Authority shall summon in writing individuals whose participation in hearing the case is necessary.

(2) In summons the Authority shall notify individuals laid down in paragraph 1 of legal consequences of non-attendance.

Section 115

Bringing before the Authority

(1) The witness who did not attend without just excuse or without substantial reasons at the Authority and without whose personal participation the Procedure cannot be carried out, may be brought before the Authority.

(2) The Authority will ask the Police to bring the witness, in case of soldiers in active service or members of armed forces their superiors will be asked.

Section 116

Procedural fine

(1) The Authority may impose a procedural fine as follows

a) any individual may be fined up to 50,000 CZK who obstructs the course of the Procedure, in particular due to non-attendance without substantial reasons at the Authority on its written notice, gives false or incomplete testimony or refuses to give testimony without reason or to submit the document;
b) any State body, legal person or natural person pursuing business may be fined up to 500,000 CZK if it or he/she does not provide free of charge the Authority with requested information needed for the security Procedure according to S. 117 par. 7.

(2) The fine according to paragraph 1 can be imposed repeatedly. The collective sum of imposed procedural fines shall not exceed the amount of 100,000 CZK in case of a fine according to paragraph 1 a), and the amount of 1,000,000 CZK in case of a fine according to paragraph 1 b).

(3) S. 156 par. 3 and 7 to 9 will be applied for determination of the rate of the fine and

for determination of its maturity, and for collection and for enforcing the payment of a fine being imposed.

280. **Time limits, computation of time and delivery**

281.

282. **Section 117**

283.

(1) The Authority shall complete the PSC Procedure within the following periods starting from the date of its initiation

284.

a) 2 months for the security classification level CONFIDENTIAL;
b) 6 months for the security classification level SECRET;
c) 9 months for the security classification level TOP SECRET.

(2) The Authority shall complete the FSC Procedure within the following periods starting from the date of its initiation

a) 6 months for the security classification level CONFIDENTIAL;
b) 8 months for the security classification level SECRET;
c) 10 months for the security classification level TOP SECRET.

(3) The Authority shall complete the Certificate Procedure within 75 days starting from the date of its initiation.

(4) The Intelligence Service concerned and the Police shall forward to the Authority findings of investigation carried out according to S. 107 par. 2, second sentence, and S. 107 par. 3 within the following periods starting from the date of delivery of its request

a) 4 months for the security classification level SECRET;
b) 6 months for the security classification level TOP SECRET.

(5) The Intelligence Service concerned and the Police shall forward to the Authority findings of investigation carried out according to S. 108 par. 5 within the following periods starting from the date of delivery of its request

285.

a) 3 months for the security classification level CONFIDENTIAL;
b) 4 months for the security classification level SECRET;
c) 6 months for the security classification level TOP SECRET.

(6) The Intelligence Service concerned and the Police shall forward to the Authority findings of investigations carried out according to S. 109 par. 2 within 2 months starting from the date of delivery of its request.

(7) The State body, legal person or the natural person pursuing business shall meet the request of the Authority for provision of information free of charge within 30 days starting from the date of delivery of the request according to S. 107, 108 or 109.

(8) If the natural person gives consent to verification of information according to S. 107 par. 5 or S. 109 par. 2 or if the facility gives consent according to S. 108 par. 7, time

limits shall apply to the procedure concerned as determined for the security classification level for acts of which the consent has been given.

Section 118

(1) If the Intelligence Service or the Police cannot notify the Authority of the results of investigation within the periods according to S. 117 par. 4 to 6 it shall inform the Authority thereof.

(2) If the State body, legal person or natural person pursuing business cannot provide information within a period as outlined in S. 117 par. 7 it shall inform the Authority thereof.

(3) If the Authority cannot make a decision due to notification according to paragraph 1 or 2 in time limits according to S. 117 par. 1 to 3, the director of the Authority will extend the period accordingly, but not more than twice, and notify in writting the participant in the Procedure thereof, giving the reasons for this extension.

(4) In single procedure as described above an extension of the time limit according to paragraph 3 shall not exceed the period required for carrying out the Procedure for the corresponding level.

Section 119

Computation of time

(1) The day on which the circumstance determining the beginning of the time limit occurred will not be included into the limit. Time limits determined according to months or years will expire on expiration of the day that conforms by its marking with the date when the circumstances determining the beginning of the time limit occurred, if there is no such date in the month, the time limit will end on the last day of the month. If the final date of the time limit falls on a weekend or holiday the next working day will be the last date of the time limit.

(2) The time limit will be observed if submission is made with the Authority at least on the last day of the time limit or if the mail addressed to the Authority has been posted on that day, which contains submission, to the postal licence holder or to the special postal licence holder or to a person holding the similar position in another state.

(3) In case of doubts the time limit shall be considered to be observed unless the contrary has been proved.

(4) When compelling reasons are present and the participant in the Procedure fails to observe the time limit, the Authority will waive the lapse of time if the participant in the Procedure applies for an extension of time within 5 days starting from the date when reasons of such a default cease to exist, and if the participant in the Procedure takes action in default within the same timeframe. The Authority may award suspensory effect to this request.

(5) No remonstrance shall be permitted against the motion to waive the lapse of time.

Section 120

298.
299. **Delivery**
300.

(1) Decisions and other documents will be delivered by the Authority itself to the data box of the participant in the Procedure or through the postal licence holder or special postal licence holder, which have the duty resulting from the postal contract to deliver documents as specified by this act. Delivery to the foreign countries shall take place through the Ministry of Foreign Affairs. In case of members or employees of armed forces and security corpses the delivery to foreign countries can take place through competent security director. All documents shall be delivered into the own hands of the recipient. If the participant in the Procedure has a representative the documents stall be delivered only to that representative; in case of personal acts the documents will be delivered also to the participant in the Procedure. The delivery to the subject being represented has no effect to running of time. If the Procedure has been terminated according to S. 113 par. 1 i) no decision will be delivered.

(2) If the addressee refuses to receive the service of the document, the postal licence holder or the special postal licence holder will mark this fact on the advice of delivery together with the date, and send the document back to the Authority. The document shall be considered to be delivered as of the date of refusal of reception of the service of the document; if the delivery takes place by the Authority, the refusal of reception of the service of document will be marked by the Authority accordingly.

(3) If the addressee has not been available at the place of delivery, although he/she resides at the place of delivery, the deliverer shall deposit the mail with the Authority or in the premises of the postal licence holder or special postal licence holder having local competence. The mail will be deposited for 10 days. The addressee shall be called on by inserting the notice into his letterbox or by another practicable manner to take the delivery. If the addressee does not take the document within 10 days from the date of its deposit, the last day of this period shall be considered as the date of delivery, even if the notification of delivery of the document did not come to the knowledge of the addressee.

(4) If the contrary is not proved by the adressee, it shall be taken that the addressee had stayed in the place of delivery.

(5) In case of the natural person the place of delivery shall be the home address in the territory of the Czech Republic indicated by that person. If the natural person stays abroad on a long-term basis in the interest of the State, the home address in the foreign country may also be the place of delivery.

(6) If the document is delivered to the addressee in a foreign country, the time limits according to this Act do not run during the time of delivery.

(7) The document may be delivered to the natural person anywhere he/she will be found. If the addressee refuses to receive the service of the document, the procedure shall apply according to
paragraph 2 accordingly.

(8) In case of a legal person the document shall be delivered to the address of its location, and in case of a natural person pursuing business the document shall be delivered to the address of his/her place of business activity. A responsible person or employee authorised

to receive documents are entitled to take delivery of the document on behalf of the legal person.

(9) Persons of unknown stay or location and persons to whom documents cannot be verfiably delivered, can be served on by public notice. Delivery by public notice shall be carried out in such a way that the document or the notice of possibility to receive the document will be posted up on the official notice board of the Authority and the date of the posting will be marked on the document. Starting from the fifteenth day from the posting the document shall be considered to be delivered if also the duty of publication according to paragraph 10 has been met within this time limit.

(10) The Authority shall establish the official notice board, which shall be permanently publicly accessible. The content of the public board is being published also on websites of the Authority.

301.

302.

303. **Decision**

304.

305. **Section 121**

306.

(1) If the Authority affirmatively disposes of the natural person application, facility application or Certificate application it will not issue the written decision. In these cases the Authority will issue the PSC, FSC or Certificate and deliver it to the participant in the Procedure; the Authority will file the copies into the security file (S. 124).

(2) If the Authority does not affirmatively dispose of the natural person application, facility application or Certificate application it will issue the decision of non-issuance of the PSC, FSC or

307. Certificate and deliver it to the participant in the Procedure; the Authority will file the copy into the

security file.

(3) If the Authority terminates validity of the PSC, FSC or Certificate it will issue a decision thereof and deliver it to the participant in the Procedure; the Authority will file the copy into the security file.

(4) In case of Procedure carried out upon request by the appropriate body of the European Union or the international organization of which the Czech Republic is the member according to S. 93 par. 1 b) the Authority will send to this body the notice of results of this Procedure.

Section 122

Elements of the decision

(1) The decision shall be issued in writing and it shall contain statements of the decision, reasoning and briefing of the participant in the Procedure. The coming into force of the decision delivered to the participant in the Procedure, who is the natural person, shall be notified immediately by the Authority to the responsible person of this participant. In case of termination of validity of the Certificate that has been issued for military material trading

according to the special legal regulation the Authority shall notify the coming into force of the decision to the Ministry of Industry and Commerce.

(2) The solution of the matter that is the subject matter of the decision-making process and provisions of this Act, under which the decision was taken, shall be given in the statements of the decision. The part of the statements of the decision shall also contain a marking of the participant in the Procedure that enables his/her/its identification. If the participant in the Procedure is the natural person, he/she shall be identified by the name, surname and by the birth registration number (personal identity number). If the participant in the Procedure is the facility, it shall be identified by the Firm or the name, company registration number and by its location. The part of statements may also contain determination of the time limit to perform imposed duty.

(3) Reasons for issuance of the decision shall be provided for in the reasoning, as well as grounds for its issuance, considerations that has been followed by the Authority in their evaluation and in application of legal regulations. If some of the reasons for issuance of the decision are classified information, then only reference to grounds for issuance of the decision and its classification level shall be quoted. Considerations that have been followed by the Authority in their evaluation and reasons for issuance of the decision will be quoted only to the extent in which they are not classified information.

(4) It shall be stated in the briefing whether remonstrance may be lodged against the decision, within what time limit, from what date this time limit will be calculated, who decides on the remonstrance, with what body it will be lodged, as well as the fact that the remonstrance has no suspensive effect.

(5) Further the decision shall contain identification of the Authority, date of its making, official stamp, name, surname, position and signature of the employee of the Authority who issued the decision.

(6) Correction of evident incorrectness in the written decision will be made by the Authority
308. anytime even without the motion and the participant in the Procedure shall be notified thereof. If the
309. correction concerns statements of the decision, the Authority shall issue an remedial decision thereof. The remonstrance may be permitted against the amended decision.
310.

Section 123

311. **Legal force and enforcement of the decision**
312.

(1) Decision shall become effective if it has been delivered and no remonstrance may be permitted against it.
313.

(2) The Authority shall mark on the decision upon request of the participant in the Procedure, when the decision has become effective.
314.

(3) The decision shall be enforceable if it has become effective or if it has been delivered and the remonstrance against it has no suspensive effect.

Section 124

315. **Security file**
316.

(1) The security file contains materials relating to the Procedure and reporting of changes; and it is subdivided into classified and unclassified parts.

(2) The security file shall be filed, kept, updated, recorded and discarded by the Authority; it will be discarded after the expiration of 15 years from the date of the last effective decision in the Procedure.

(3) The data in the security file may be used only for the needs of fulfilment of duties according to this Act.

(4) Employees of the Authority who carry out the Procedure shall keep confidential the data entered in the security file that came to their knowledge during carrying out this Procedure or in connection with it even after termination of their labour-law relations.

(5) Upon request by investigative, prosecuting and adjudicating bodies the director of the Authority may relieve individuals outlined in paragraph 4 from obligations to maintain confidentiality.

CHAPTER III

317. **Remonstrance and judicial review**
318.

319. **Basic provisions, time limits for lodging the remonstrance and its elements**
320.
321. **Section 125**
322.

323. The participant in the Procedure shall have the right to lodge the remonstrance against the decision of the Authority issued in the Procedure, unless he/she/it has waived this right in writing or unless otherwise provided herein.
324.
325.
326. **Section 126**
327.

(1) The remonstrance will be lodged with the Authority within 15 days from the date of delivery of the decision.

(2) In case of missing, incomplete or mistaken briefing the remonstrance may be lodged within 3 months from the date of delivery of the decision.

(3) The Authority will waive the lapse of time for lodging the remonstrance when compelling reasons are present and when the participant in the Procedure makes request within 15 days starting from the date when reasons of such default cease to exist and the participant in the Procedure lodges the remonstrance simultaneously.

(4) Lodging of the remonstrance against the decision to terminate the validity of the PSC, FSC or Certificate has no suspensive effect.

(5) If the participant in the Procedure has withdrawn the remonstrance in writing after expiry of the time limit according to paragraph 1, he/she/it cannot lodge it again.

Section 127

(1) The remonstrance lodged by the natural person shall contain his/her name, surname, birth registration number (personal identity number) and address of permanent residence or delivery address, it shall be dated and signed.

(2) The remonstrance lodged by the legal person pursuing business shall contain its identification by the Firm or name and company registration number and address of its location or another delivery address. The remonstrance shall be dated and signed by a person or persons who are authorised to act for the facility.

(3) It shall be further stated in the remonstrance against what decision it is aimed, what the participant in the Procedure seeks and what is considered to be contrary to legal regulations, or other incorrectness of the contested decision. No remonstrance shall be permitted only against the reasoning of the decision.

(4) If the remonstrance has not the requested elements, the Authority shall request the subject lodging the remonstrance to eliminate deficiencies. It shall determine the time limit in its request for elimination of deficiencies that may not extend beyond 15 days and brief him/her/it of legal consequences if these deficiencies are not eliminated [S. 113 par. 1 c)].

Practice of the Authority before the decision of the director of the Authority

Section 128

(1) The Authority will dismiss the remonstrance by its decision, without signing its decision by the director of the Authority, if

a) the remonstrance cannot be lodged according to this Act; or
b) the remonstrance has been lodged after the time limit determined according to S. 126 par. 1, unless the default of time for its lodging has been waived according to S. 126 par. 3.

(2) The remonstrance may be permitted against the decision provided for in paragraph 1.

Section 129

(1) The Authority may decide the remonstrance itself, without signing its decision by the director of the Authority, if it allows the remonstrance completely; if the Authority allows the remonstrance, it will cancel the contested decision.

341.

(2) The remonstrance may be permitted against the decision provided for in paragraph 1.

(3) If the Authority does not decide the remonstrance according to paragraph 1 or according
342. to S. 128, it will forward it with its opinion and with all documentary files, within 15 days from the date of delivery of the remonstrance, to the director of the Authority.

343. **Decisions of the director of the Authority in the procedure to deal with the remonstrance**

344.

345. **Section 130**

346.

(1) The remonstrance will be decided by the director of the Authority upon a motion of the
347. remonstrance commission, unless the procedure according to S. 128 par. 1 or S. 129 par. 1 is not applied.

(2) Members of the remonstrance commission shall be appointed and removed by the director of the Authority. The remonstrance commission shall have at least 5 members. More then half of the members of the commission shall have a university legal education. The member of the remonstrance commission shall be a holder of valid PSC and a national of the Czech Republic. The remonstrance commission shall always be established for a period of 5 years; the chairman of the remonstrance commission shall always be one of the members of this commission for a period of one calendar year. The remonstrance commission is able to act if more than a half of its members are present; the resolution will be adopted by more than half of votes of its members being present.

(3) The majority of members of the remonstrance commission shall be employees of the State assigned in other State bodies than in the Authority; it does not apply to the structure of the remonstrance commission in the procedure according to S. 140 par. 1 a).

(4) Membership in the remonstrance commission shall be terminated

a) upon expiration of the term of office of this commission;
b) upon discharge from the position;
c) upon resignation;
d) upon death or declaration of death of a person.

(5) The member of the remonstrance commission is not entitled to the remuneration. The Authority can reimburse travelling expenses to members of the remonstrance commission in accordance with the Act regulating travelling reimbursements.

Section 131

(1) The director of the Authority shall terminate the procedure to deal with the remonstrance if grounds exist according to S. 113, and cancel the contested decision if the

decision has become faint due to the termination of the procedure; or else he/she will confirm the contested decision.

(2) The contested decision will be cancelled by the director of the Authority if he/she allows

348. completely the remonstrance lodged against the decision to terminate validity of the PSC, FSC or Certificate.

(3) The director of the Authority shall cancel the contested decision and refer the case back to the new consideration and decision if

a) a contested decision has been issued contrary to legal regulations or is erroneous in another way; or
b) it has been determined that circumstances have arisen after the issuance of the decision that have a bearing on the decision.

(4) The remonstrance shall be dismissed and the decision confirmed by the director of the Authority if he/she does not find any reason for measures according to paragraphs 1 to 3.

(5) In the reasoning of decision on the remonstrance according to paragraph 3 the director of the Authority shall also deliver a legal opinion by which the Authority shall be bound in the new hearing of the case, unless this legal opinion becomes faint due to a change of the legal status or factual circumstances. In the new Procedure the Authority may use grounds of the original decision including grounds of the decision on remonstrance, unless it is contrary to the grounds for the new Procedure. The remonstrance may be permitted against the decision issued in the new Procedure, unless otherwise provided herein.

(6) The director of the Authority shall decide the remonstrance within 3 months from the date of delivery of the remonstrance.

349. **Section 132**
350.

351. Validity of the PSC, FSC or Certificate will be renewed as of the date of legal effect of the decision on remonstrance according to S. 129 par. 1 or S. 131 par. 2 or 3, which has been terminated as a result of the contested decision. Together with the decision on remonstrance the PSC, FSC or Certificate will be sent back to the participant in the Procedure that has been forwarded according to S. 66 par. 1 b), S. 68 a) or S. 87 par. 1 a); the validity period of the security clearance or Certificate shall be maintained.
352.
353.
354.
355.
356.
357.

CHAPTER IV

Judicial review and final provision

Section 133

(1) An action can be brought against the decision of the director of the Authority according to the special legal regulation within 30 days of the service of the decision. Where the decision of the director of the Authority according to S. 131 par. 1 is in question, the action can be brought only if remonstrance is allowed to be lodged against the grounds to terminate the Procedure according to S. 113 par. 5.

(2) Facts at the judicial proceedings shall be introduced in evidence in such a way so as not to affect the duty to maintain confidentiality concerning classified information contained in results of an investigation or in the data from records of the Intelligence Services or the Police. Evidence by examination concerning these factors may be produced only if the person who has obligation to maintain confidentiality has been released from that obligation by the competent authority; the release from obligation to maintain confidentiality is not possible only in cases when threat could arise that may endanger or seriously affect activities of the Intelligence Services or the Police; an appropriate procedure will also be followed in cases where evidence is not produced by examination.

(3) The Authority shall mark factors set out in paragraph 2 in respect to which it claims that nobody can be released from the obligation to maintain confidentiality, and the judge presiding over the case shall decide that parts of the file to which these factors apply will be separated if the activities of the Intelligence Services or of the Police could be endangered or seriously affected; separated parts of the file cannot be inspected by the participant in the Procedure, by his/her representative as well as by the person participating in the Procedure. Provisions of the special legal regulation relating to the evidence, marking of parts of the file and its inspection shall be without prejudice to any other facts than those specified above.

Section 134

358. Save as otherwise provided for in paragraphs 125 to 132, appropriate provisions of paragraphs 89 to 124 shall be used accordingly for the procedure to deal with the remonstrance.

CHAPTER V

Delegating provisions

Section 135

359. The implementing legal regulation shall determine

a) the format of briefing according to S. 58 par. 5;
b) the formats and way of making applications according to S. 93 par. 1 a);
c) the extent and form of documents according to S. 94 par. 2 b);
d) the extent of data of the personnel questionnaire in case of an application according to S. 94 par. 5, the questionnaire in case of an application according to S. 99 par. 5, the extent of data of the facility questionnaire in case of an application according to S. 96 par. 5;
e) the format of the statement of personnel eligibility;

f) the format of the personnel questionnaire according to S. 95;
g) the extent and form of documents according to S. 96 par. 2 c) and their elements and the format of the facility questionnaire according to S. 97; and
h) the extent and form of documents according to S. 99 par. 2 c) and the format of the questionnaire according to S. 100;
i) the extent of written justification according to S. 94 par. 1, S. 96 par. 1 and S. 99 par. 2 d);
j) limitation of the extent of reports on changes to data, as well as the manner and form of their proving, according to S. 66 par. 1 d), S. 68 c) and d), S. 87 par. 1 c) and S. 103 par. 2;
k) the format of statement of release from confidentiality according to S. 94 par. 2 g), S. 96 par. 2 d) and S. 99 par. 2 d).

360.

361. **PART FIVE**
362.
363. **EXERCISE OF THE STATE**
364. **ADMINISTRATION**

Section 136

(1) The state administration in the areas of protection of classified information and security
365. eligibility shall be exercised by the Authority, save as otherwise provided herein.

(2) The Authority is headed by the director who shall be appointed by the government, after
366. consideration in the committee of the Chamber of Deputies in charge of the security matters, and the director will also be removed by the government.

(3) The director of the Authority shall be answerable to the Prime Minister or to the authorized member of the government.

Section 137

The Authority

367. The Authority as the central administrative authority shall

a) decide the natural person application, facility application and Certificate application, as well as termination of validity of the PSC, FSC and Certificate, with the exception of cases set out herein [S. 140 par. 1 a) and S. 141 par. 1] and issue Personnel security clearance according to S. 56a;
b) carry out the state supervision in areas of protection of classified information and security eligibility (S. 143) and methodical activities, with the exception of cases set out herein [S. 143 par. 5);
c) ensure specialist competence exams and issue a Specialist Competence Certificate;

d) perform tasks in the area of protection of classified information in accordance with obligations arising out of membership of the Czech Republic in the European Union, North Atlantic Treaty Organization and arising out of international agreements by which the Czech Republic is bound;
e) keep the Central Registry and approve establishment of registries in the State bodies and in facilities;
f) permit in determined cases providing classified information within the scope of international relations;
g) issue courier certificates upon written request of the responsible person or security director for the purposes of courier transportation of classified information classified at security classification levels TOP SECRET, SECRET or CONFIDENTIAL to be provided within the scope of international relations, with the exception of classified information provided according to S. 78 par. 1, and arrange for its transportation in justified cases;
h) ensure activities of the National Communication Security Agency, National Cryptographic Material Distribution Agency, National Compromising Electromagnetic Emissions Measurement Agency and National Information Systems Security Agency, which are its parts;
i) carry out certification of technical means, Information System, cryptographic device, cryptographic site and shielded chamber and approve the Communication System security project;
j) ensure research, development and production of national cryptographic devices;
k) develop and approve national cipher algorithms and create national cryptographic protection policy;
l) investigate compromising emissions where classified information is present or its future occurence is excpected;
m) examine in co-ordination with the Intelligence Services and with the Police those areas where meetings are held to ensure that no threats to classified information arise and no leakage of classified information takes place as a result of unauthorized use of technical means intended for obtaining information;
n) makes security standards;
o) impose sanctions for breach of duties as described herein;
p) decide other subject-matters and fulfil other tasks in the areas of protection of classified information and security eligibility as described herein;
q) issue the Bulletin of the Authority, which is published on its websites.

Section 138

(1) In fulfilment of tasks according to this Act the Authority shall be entitled

a) to process personal data to the extent necessary for fulfilment of tasks according to this Act;
b) to keep records of breach of protection of classified information, records of security directors (security officers), records of natural persons and facilities having access to classified information, with the exception of members and employees assigned to the Intelligence Services and selected policemen, records of natural persons who are holders of the Certificate, records of cryptographic protection staff, couriers of the cryptographic material and records of natural persons who are holders of the Specialist Competence Certificate;

c) to keep a certification file of the Information System, cryptographic device, cryptographic site and of the shielded chamber, to keep list of cryptographic items being controlled and to keep documentation governing activities according to S. 45;
d) to require provision of information from the State body, legal person or the natural person pursuing business free of charge, and to use and record this information;
e) to require, for the purposes of the Procedure, from the Police and from the Intelligence Services information obtained by procedures according to the special legal regulation;
f) to require a copy of criminal conviction records; the request for issuance of a copy of criminal conviction records and a copy of criminal conviction records shall be provided in electronic form in a manner making the remote access possible;
g) to inspect the criminal files, to make abstracts and copies thereof;
h) to provide to the State body, legal person or natural person pursuing business to the extent necessary the requisite personal data relating to the information being requested;
i) to make a contract with the State body or facility to carry out partial tasks in certification of technical means, Information Systems, cryptographic devices, cryptographic site, shielded chambers, to carry out training aimed at the specific specialist competence of the cryptographic protection staff and to investigate the possibility of occurrence of compromising emissions where classified information will be present, and to produce cryptographic devices;
j) to maintain data within its Information Systems obtained in the conduct of duties in accordance with this Act;
k) to co-operate with the authority of the foreign power during the security clearance procedure having the jurisdiction in the area of protection of classified information, in particular to require information concerning the participant in the Procedure;
l) to express its opinion to notification according to S. 69 par. 1 r) within 30 days from the date of its delivery and to provide summary of these notifications and of statements with respect to them to the Office for the Protection of Competition; and
m) to perform acts according to S. 107 par. 1 for the purpose of deciding by the Office for Foreign Relations and Information and of the Military Intelligence according to S. 140 par. 1, upon their written request.

(2) Once a month the Authority shall provide to the Intelligence Services and to the Ministry of the Interior a list of
368.
a) issued PSCs, FSCs and Certificates;
b) natural persons in respect of whom it decided not be issued with the public instrument outlined under bullet a) or of persons in respect of whom the validity of this instrument has been terminated;
c) facilities in respect of which it has received the Statement of Facility according to S. 15a par. 2 or 3.

Section 138a

(1) For the purposes of execution of responsibilities in accordance with this Act the Authority shall be provided with reference data from the basic register of citizens as follows

a) surname;
b) name or names;
c) residence address;
d) date, place and district of birth; in case of subject of data, which was born abroad, date, place and state of birth;
e) date, place and district of death; in case of subject of data, which died outside the territory of the Czech Republic, date of death, place and state on the territory of which the death occured;
f) citizenship or more citizenships if applicable.

(2) For the purposes of execution of responsibilities in accordance with this Act the Authority shall be provided with data concerning nationals of the Czech Republic from the agenda information system of the register of citizens as follows

a) name or names, surname including previous surnames, maiden (sur)name;
b) male or female;
c) birth registration number (personal identity number), date of birth if this was not assigned;
d) permanent residence address including previous permanent residence adressess or mailing address for delivery of documents according to other legal regulation;
e) beginning of permanent residence or the date of cancellation of data concerning the place of permanent residence or the date of termination of permanent residence in the territory of the Czech Republic;
f) judicial incapacitation or limitation of legal capacity, name or names, surname and birth registration number (personal identity number) of a guardian; if no birth registration number (personal identity number) has been assigned to the gaurdian, date, place and district of birth; if the body of local government has been appointed as the guardian, name and address of its office;
g) name or names, surname and birth registration number (personal identity number) of father, mother or of other statutory representatives; if no birth registration number (personal identity number) has been assigned to one of parents or to other statutory representative name or names, surname, date of birth; if a legal person presents other statutory representative of a child the name and address of its office;
h) family status, date, place and district of contracting of marriage, if the marriage has been contracted outside the territory of the Czech Republic place and state, date of coming into force of decision of court on declaring the marriage void, date of coming into force of decision of court on non-existence of marriage, date of termination of marriage due to death of one of the spouses or date of coming into force of decision of court on declaration of death of one of the spouses, as well as the date stated in final decision of the court on declaration of death of one of the spouses as the day of death or as the day which one of the spouses declared dead did not survive, or date of coming into force of decision of court on divorce;
i) date and place of contracting of registered partnership, date of coming into force of decision of court on declaring the registered partnership void or date of coming into force of decision of court on non-existence of registered

partnership, date of termination of registered partnership due to death of one of the registered partners or date of coming into force of decision of court on declaration of death of one of the registered partners, as well as the date stated in final decision of the court on declaration of death as the day of death or as the day which one of the partners declared dead did not survive, or date of coming into force of decision of court on termination of registered partnership;

j) name or names, surname including previous surnames and birth registration number (personal identity number) of the spouse or registered partner; if the spouse or registered partner is a natural person with no birth registration number (personal identity number) assigned, name or names, surname of the spouse or registered partner and date of his/her birth;

k) name or names, surname and birth registration number (personal identity number) of the child; if the child is a foreigner with no birth registration number (personal identity number) assigned, name or names, surname of the child and date of its birth;

l) concerning adopted child to the following extent

1. degree of adoption;
2. original and new name or names of the child;
3. original and new birth registration number (personal identity number) of the child;
4. date, place and district of birth;
5. birth registration numbers (personal identity numbers) of adoptive parents, if the adoptive parent has no birth registration number (personal identity number) assigned, data concerning name or names, surname and data of birth of the child;
6. birth registration numbers (personal identity numbers) of mother and father; if they have no birth registration number (personal identity number) assigned, their name or names, surname and date of birth;
7. date of coming into force of decision on adoption or decision on cancellation of adoption order of the child;

m) date, place and district of death; in case of a citizen who died outside the territory of the Czech Republic, date of death, place and state on the territory of which the death occured;

n) day that was declared as a day of death in the decision of the court on declaration of death or as a day which the citizen declared dead did not survive.

The data kept as reference data in the basic register of citizens will be used from the agenda information system of the register of citizens only if it is in the form preceding the current state

(3) For the purposes of execution of responsibilities in accordance with this Act the Authority shall be provided with data concerning foreigners from the information system of foreigners as follows

a) name or names, surname, maiden (sur)name;

b) date of birth;

c) male or female;

d) place and state where the foreigner was born; if the foreigner was born in the territory of the Czech Republic place and district of birth;
e) birth registration number (personal identity number);
f) citizenship or more citizenships if applicable;
g) type of residence and residence address;
h) number and validity of residence permit;
i) beginning of residence or date of termination of residence;
j) judicial incapacitation or limitation of legal capacity;
k) administrative banishment and period for which the entry at the territory of the Czech Republic shall not be made possible;
l) family status, date and place of contracting of marriage, date of coming into force of decision of court on declaring the marriage void, date of coming into force of decision of court on non-existence of marriage, date of termination of marriage due to death of one of the spouses or date of coming into force of decision of court on declaration of death of one of the spouses, as well as the date stated in final decision of the court on declaration of death as the day of death or as the day which one of the spouses declared dead did not survive, or date of coming into force of decision of court on divorce;
m) date and place of contracting of registered partnership, date of coming into force of decision of court on declaring the registered partnership void or date of coming into force of decision of court on non-existence of registered partnership, date of termination of registered partnership due to death of one of the registered partners or date of coming into force of decision of court on declaration of death of one of the registered partners, as well as the date stated in final decision of the court on declaration of death as the day of death or as the day which one of the partners declared dead did not survive, or date of coming into force of decision of court on termination of registered partnership;
n) name or names, surname of the spouse or registered partner and his/her birth registration number (personal identity number); if the the spouse or registered partner is a foreigner with no birth registration number (personal identity number) assigned, name or names, surname and date of its birth;
o) name or names, surname of child if the child is a foreigner according to other legal regulation, and its birth registration number (personal identity number); if no birth registration number (personal identity number) has been assigned to the child name or names, surname and date of its birth;
p) name or names, surname of father, mother or of other statutory representative if they are foreigners according to other legal regulation, and their birth registration number (personal identity number); if no birth registration number (personal identity number) has been assigned to one of parents or to other statutory representative name or names, surname and date of birth;
q) concerning adopted child, if the child is a foreigner according to other legal regulation;

1. degree of adoption;
2. original and new name or names, surname of the child;
3. original and new birth registration number (personal identity number) of the child;
4. date and place of birth;
5. birth registration numbers (personal identity numbers) of adoptive parents, if the adoptive parent has no birth registration number (personal identity

number) assigned, data concerning name or names, surname and data of birth of the adoptive parent;

6. birth registration numbers (personal identity numbers) of mother and father; if they have no birth registration number (personal identity number) assigned, data on their name or names, surname and date of birth; these data will not be provided in case of a child born to a woman with permanent residence in the Czech Republic who gave birth to the child and applied in writting for concealment of her real ID in connection with childbirth;
7. date of coming into force of decision on adoption or decision on cancellation of adoption order of the child;

r) administrative banishment and period for which the entry at the territory of the Czech Republic shall not be made possible;

s) date, place and district of death; in case of death outside the territory of the Czech Republic state on the territory of which the death occured, or date of death;

t) the date stated in final decision of the court on declaration of death as the day of death or as the day which the foreigner declared dead did not survive;

u) name or names, surname concerning

1. dependant child of full age of a foreigner having residency permit for the territory of the Czech Republic;
2. a foreigner under full age that has been placed in the custody in the form of substitute family care to a foreigner having residency permit for the territory of the Czech Republic or to his/her spouse by decision of the competent autority or that has been adopted by a foreigner having residency permit for the territory of the Czech Republic or by his/her spouse or whose guardien or spouse of his/her guardien is a foreigner having residency permit for the territory of the Czech Republic;
3. single foreigner above 65 years of age or foreigner, irrespective of the age of the foreigner, who is not self-sufficient for health reasons, in case of family reunification with a parent or child having residency permit for the territory of the Czech Republic;
4. a foreigner who is unprovided direct relative in ascendent or descendent lines or who is such relative of a spouse of the citizen of the European Union;
5. parents of a foreigner under full age who have been granted asylum according to special legal regulation and his/her birth registration number (personal identity number); in case of foreigners who have no birth registration number (personal identity number) assigned, name or names, surname and date of birth;

The data kept as reference data in the basic register of citizens will be used from the information system of foreigners only if it is in the form preceding the current state

(4) For the purposes of execution of responsibilities in accordance with this Act the Authority shall be provided with data from the register of birth registration numbers (personal identity numbers) concerning natural persons to whom birth registration number (personal identity number) was assigned but who are not kept in the agenda information system of the register of citizens as follows

a) name or names, surname or maiden name;
b) birth registration number (personal identity number);
c) the original birth registration number (personal identity number) if the birth registration number (personal identity number) has changed;
d) day, month and year of birth;
e) place and district of birth; in case of natural person born abroad the state on the territory of which the natural person was born.

(5) In addition to data according paragraphs from 2 to 4 kept in agenda information systems the Authority shall also be provided with its preceding changes.

(6) From data being provided only such data can always be used in the specific case which is necessary to accomplish a particular task.

Section 139

(1) The Authority shall process the proposal of the list of classified information. The list of classified information will be issued by the government by its decree.

(2) The list of classified information shall classify the respective classified information into one or more security classification levels according to S. 4.

Section 140

369. **Intelligence Services**

(1) Intelligence services shall

a) decide natural person applications of its members, employees and candidates for service or employment relationship, with the exception of candidates for service or employment relationship who are holders of the PSC at least for the required security classification level, and decide the termination of validity of the security clearance of this natural person and issue security clearance of the natural person according to S. 56a;
b) carry out acts upon the written request of the Authority within its jurisdiction during the course of the Procedure according to this Act.

(2) In deciding according to paragraph 1 the Intelligence Services shall have the position of the Authority and the responsible person of the Intelligence Service shall have the position of the director of the Authority. The competence for acts shall be in accordance with S. 5 of the Act N. 153/1994 Coll., to make provisions for the Intelligence Services of the Czech Republic, as amended.

(3) In performance of duties according to this Act the Intelligence Services shall report to the Authority without delay, whenever they discover circumstances indicating that the PSC holder, FSC holder or Certificate holder no longer meets conditions for its issuance, provided that this notification will not endanger the interests pursued by the Intelligence Service.

(4) In conducting duties according to this Act the Intelligence Services shall be entitled
370.

a) to use means for obtaining information according to the special legal regulations;
b) to use data from their own records and data from records provided by the Authority;
c) to require and use data from records and materials developed in connection with activities of security and military bodies of the Czechoslovak state;
d) to process personal data;
e) to keep records;
f) to require, free of charge, information from the State body, legal person or natural person pursuing business and to use it;
g) to require a copy and extract of criminal conviction records; the request for issuance of a copy or extract of criminal conviction records and a copy and extract of criminal conviction records shall be provided in documentary or in electronic forms in a manner making the remote access possible;
h) to maintain data in the Information Systems obtained in the conduct of duties in accordance with this Act;
i) to implement measures relating to the register protection of personal data of the natural person; and
j) to use data from the register of individuals who have been granted access to classified information according to S. 58 par. 4.

(5) The public administration autority, which is administrator of information system processing relevant personal information shall render assistance to the Intelligence Services necessary to implemant measures according to paragraph 4 i).

(6) The director of the Intelligence Service gives consent according to S. 59 par. 3.

Section 141

Ministry of the Interior and the Police

(1) The Ministry of the Interior shall decide the natural person application in case of members of the Police selected in the interest of performance of important tasks of the Police by the Interior Minister with the exception of members of the Police who are PSC holders at least for the required security classification level, as well as the termination of validity of the PSC in case of these members of the Police and issue PSC according to S. 56a.

(2) In deciding according to paragraph 1 the Ministry of the Interior shall have the position of the Authority and the Interior Minister shall have the position of the director of the Authority.

(3) In performance of duties according to this Act the Ministry of the Interior shall further

a) notify the Authority without delay, whenever it discovers circumstances indicating that the PSC holder, FSC holder or Certificate holder no longer meets conditions for its issuance; and

b) implement, upon request of the Authority, measures relating to the register protection of personal data of the PSC holder or of his/her spouse, children and parents.

(4) In performance of duties according to paragraphs 1 to 3 the Ministry of the Interior shall be entitled

a) to use data from its registers as well as data provided by the Authority from its registers;
b) to process personal data;
c) to keep records;
d) to require, free of charge, information from the State body, legal person or natural person pursuing business and to use it;
e) to require an opinion of the Police on the security eligibility of the selected member of the Police;
f) to require a copy and extract of criminal conviction records; the request for issuance of a copy or extract of criminal conviction records and a copy and extract of criminal conviction records shall be provided in documentary or in electronic forms in a manner making the remote access possible;

(5) The Police shall participate, within its competence according to the special legal regulation, in performance of duties of the Ministry of the Interior according to paragraph 1; upon written request of the Authority it shall also carry out acts within its competence during the course of the Procedure.

(6) In performance of duties according to this Act, the Police shall be entitled to use data from the register of individuals granted access to classified information according to S. 58 par. 4.

(7) The public administration autority, which is administrator of information system processing relevant personal information shall render assistance to the Ministry of the Interior necessary to implemant measures according to paragraph 3 b).

(8) The Interior Minister gives consent according to S. 59 par. 3.

Section 142

(1) If any Document Found according to S. 65 par. 1 or Certificate found according to S. 87 par. 2 has been handed over to the Authority, to the Police or to the Embassy of the Czech Republic, the body concerned shall make written record of its handing over, in which it shall identify the Document or Certificate Found, and it shall insert the name, surname, birth registration number (personal identity number) and the place of permanent residence of an individual who handed over the Document or Certificate Found, and, in detail, under what circumstances the individual concerned has obtained them. The Police or Embassy of the Czech Republic shall hand over the Document or Certificate Found to the Authority together with the drawn up record. The Authority shall forward classified information to its originator, and the PSC, FSC, Certificate, PSC for the foreign power, FSC for the foreign power shall be forwarded to the person or facility concerned.

(2) For the purposes of handing over of classified information according to paragraph 1, the member of the Police or the employee working on the Embassy of the Czech Republic shall be considered to be authorized to have access to classified information to the extent necessary for making the record and for the delivery of this classified information to the Authority.

PART SIX

OVERSEEING STATE CONTROL

Section 143

(1) State control in the areas of protection of classified information and security eligibility means supervising how the State bodies, legal persons, natural persons pursuing business and natural persons (hereinafter "the Controlled Persons") comply with legal regulations in this area.

(2) In performance of the state control the procedure shall be in accordance with the Act regulating the state control, as appropriate, save as otherwise provided herein.

(3) In performance of the state control the employees of the Authority (hereinafter "the Control Staff") shall have access to classified information to the extent of the control being performed, if they prove that they have been issued with the valid PSC for the appropriate security classification level.

(4) The authority of the foreign power having jurisdiction over the protection of classified information shall be entitled to participate in the state control in the area of protection of classified information released by this authority to the Czech Republic, if this results from the obligation of the membership of the Czech Republic in the European Union, or if provided by the international agreement by which the Czech Republic is bound.

(5) In cases according to S. 141 activities of the Intelligence Services and of the Ministry of the Interior shall not be subject to the state control as described herein.

Section 144

Remedial, corrective or disciplinary measures

(1) Further to authorization according to the Act regulating the state control, if the breach of legal regulations is ascertained in the areas of protection of classified information and security eligibility of the Controlled Person, the Control Staff are authorized to adopt necessary measures to ensure the protection of classified information, including withdrawal of classified information, measures to declassify or change the level of classified information or to mark classified information with the security classification level. The certificate of withdrawal shall be issued to the Controlled Person. The Control Staff are also authorized to require that remedial or corrective actions shall be taken within a prescribed period to correct any deficiency being discovered.

(2) Costs of implementation of measures according to paragraph 1 shall be met by the Controlled Person.

(3) In conducting necessary measures according to paragraph 1 instructions of the Control Staff shall be complied with by each person.

(4) The Authority can impose a procedural fine for non-compliance with obligations according to paragraph 3 up to 100,000 CZK. The procedural fine can be imposed repeatedly. A collective sum of imposed procedural fines shall not exceed the amount of 400,000 CZK. S. 156 par. 3 and 7 to 9 will be applied for determination of the rate of the fine and of its maturity, and for collection and enforcing the payment of imposed fines.

PART SEVEN

CONTROL OVER ACTIVITIES OF THE AUTHORITY

Section 145

(1) Control over activities of the Authority shall be performed by the Chamber of Deputies that shall establish the special control body for this purpose (hereinafter "the Control Body").

(2) The Control Body shall be composed of 7 members. Only a deputy of the Chamber of Deputies may be a member of the Control Body.

(3) The special legal regulation shall apply, as appropriate, to discussions of the Control Body and to rights and obligations of its members, save as otherwise provided for in this Act.

(4) The members of the Control Body shall be permitted escorted access to the facilities of the Authority if accompanied by the director of the Authority or by an employee authorized by him/her.

(5) The director of the Authority shall submit to the Control Body

a) the report on activities of the Authority;
b) the report on individual Procedures with respect to the natural person application, facility application and Certificate application and on the termination of validity of a PSC, FSC or Certificate [S. 137 a)];
c) the draft budget of the Authority;
d) grounds necessary for the budgetary control of the Authority;
e) internal regulations of the Authority.

(6) The Control Body has no authorization to interfere with the personal competences of chief officers of the Authority and to substitute their management activities.

Section 146

(1) If the Control Body considers that the activity of the Authority unlawfully restricts or infringes on the rights and liberties of citizens, or that decision-making activity of the

Authority in the conduct of the security clearance procedure is affected by mistakes, it is entitled to ask for a necessary explanation from the director of the Authority.
390.

(2) The notification shall be given to the director of the Authority and to the Prime Minister by the Control Body, of any breach of the law by an employee of the Authority in fulfilment of obligations according to this Act, which was discovered in conducting its control activities.

Section 147

391. The obligation to hold information in confidence imposed on members of the Control Body under this Act does not apply to cases when the Control Body submits notification according to S. 146 par. 2.
392.
393.

394. **PART EIGHT**

395.

ADMINISTRATIVE DELICTS

Section 148

(1) The natural person commits an administrative infraction if

a) as the participant in the security clearance procedure does not notify the change to the data contained in the natural person application according to S. 103 par. 2, or to the data contained in the Certificate application according to S. 103 par. 2;
b) does not hand over the Document Found according to S. 65 par. 1 or Certificate found according to S. 87 par. 2;
c) breaches the obligation to hold classified information in confidence;
d) allows access to classified information to an unauthorized person;
e) carries out functions of the security director (security officer) contrary to S. 71 par. 5 with more State bodies or facilities;
f) conducts cryptographic protection without being a member of the cryptographic protection staff fulfilling conditions as set out in S. 38 par. 2;
g) operates the cryptographic device without meeting requirements as set out in S. 40 par. 2;
h) transports cryptographic material without being the courier of the cryptographic material that meets requirements as set out in S. 42 par. 1;
i) gains access to classified information without meeting the conditions according to S. 6 par. 1 or S. 11 par. 1; or
j) leaves the territory of the Czech Republic with the certified cryptographic device without permission of the Authority.

(2) Fines can be imposed for administrative infractions up to

a) 50,000 CZK in case of an administrative infraction according to paragraph 1 a);
b) 100,000 CZK in case of an administrative infraction according to paragraph 1 b) or e);

c) 500,000 CZK in case of an administrative infraction according to paragraph 1 f), g) or h);
d) 1,000,000 CZK in case of an administrative infraction according to paragraph 1 i);
e) 5,000,000 CZK in case of an administrative infraction according to paragraph 1 c), d) or j).

396.
397. **Section 149**

(1) The natural person with access to classified information commits an administrative infraction if he/she

a) does not register or does not record classified information in administrative aids according to S. 21 par. 5;
b) makes a reproduction, copy or translation of classified information without consent as outlined in S. 21 par. 6;
c) hands over classified information contrary to S. 21 par. 8;
d) lends, transports or carries classified information contrary to S. 21 par. 7 or 9;
e) declassifies classified information or changes its security classification level without consent of the originator or of the foreign power providing information;
f) does not meet the conditions for processing or storing classified information according to S. 24 par. 5 or 6;
g) handles classified information in the Information System that has not been certified by the Authority or has not been certified for the respective security classification level or has not been approved in writing for operation by the responsible person or by a person authorized by the responsible person;
h) handles classified information in the Communication System, the security project of which has not been approved by the Authority or which has not been approved for the security classification of classified information sent;
i) processes classified information contrary to security operation guidelines issued according to S. 36 par. 2;
j) does not keep records of cryptographic material in administrative aids of the cryptographic protection; or
k) handles cryptographic material contrary to S. 41 par. 2 or 3.

(2) Fines can be imposed for administrative infractions up to

a) 500,000 CZK in case of an administrative infraction according to paragraph 1 a), b), c), d), e), f), g) or h);
b) 1,000,000 CZK in case of an administrative infraction according to paragraph 1 i), j) or k).

Section 150

(1) The natural person who is a holder of the PSC commits an administrative infraction if he/she

a) does not hand over the invalid PSC according to S. 66 par. 1 b);
b) does not report the loss or theft of the PSC according to S. 66 par. 1 c);

c) does not report without delay a change to the data entered in the natural person application according to S. 66 par. 1 d);
d) does not hand over, as a holder of the PSC for the foreign power, the invalid PSC for the foreign power according to S. 57 par. 8; or
e) does not report, as a holder of the PSC for the foreign power, loss or theft of the PSC for the foreign power according to S. 66 par. 1 c).

(2) The fine of up to 50,000 CZK can be imposed for an administrative infraction according to paragraph 1.

Section 151

(1) A natural person who is a holder of the Notice commits an administrative infraction if he/she

a) does not report the change of conditions for issuance of the Notice as outlined in S. 6 par. 2 a) and c) or change to the data entered in the Notice;
b) does not hand over the invalid Notice according to S. 9 par. 6.

(2) A fine of up to 30,000 CZK can be imposed for an administrative infraction according to paragraph 1.

Section 152

(1) A natural person who is a holder of the Certificate commits an administrative infraction if he/she

a) does not hand over the invalid Certificate according to S. 87 par. 1 a);
b) does not report the loss or theft of the Certificate according to S. 87 par. 1 b); or
c) does not report the change to the data entered in the Certificate according to S. 87 par. 1 c) or to the data in the Certificate application according to S. 87 par. 1 c).

(2) The fine of up to 50,000 CZK can be imposed for an administrative infraction according to paragraph 1.
398.
399.
400. **Section 153**
401.
(1) A legal person or natural person pursuing business with access to classified information or a State body commits an administrative infraction if he/she/it
402.
a) does not provide the guards at the premises housing the security area of the category RESTRICTED, according to S. 28 par. 2 or 4;
b) does not publish security operation guidelines contrary to S. 36 par. 2;
c) does not secure the written authorization of the natural person to have access to classified information subject to Special Handling Regime, marked as “ATOMAL”;

d) does not establish and staff a position of the security director (security officer) according to S. 71 par. 1;
e) does not report an appointment to the office of the security director (security officer) according to S. 71 par. 2;
f) does not mark elements on classified information according to S. 21 par. 2 to 4;
g) as the originator, marks the security classification level on the information that is not included on the list of classified information, or on information whose divulgence or misuse cannot cause damage to the interests of the Czech Republic or cannot be unfavourable to these interests;
h) as the originator, does not report declassification or change of the classification level according to S. 22 par. 6;
i) as the addressee of classified information, does not report declassification or change of the classification level according to S. 22 par. 6;
j) does not provide continuing guards at the premises according to S. 28 par. 1, 3 or 4 housing the security area or the meeting area;
k) does not report the breach of obligations in the protection of classified information;
l) does not prepare the physical security project according to S. 32;
m) does not keep some of records/files as outlined in S. 69 par. 1 j);
n) does not hand over classified information to be recorded according to S. 69 par. 1 n);
o) does not ensure that implemented measures of physical security correspond with the physical security project and requirements set out according to S. 31;
p) as the originator, does not mark the elements according to S. 21 par. 1 and 4, although the information is included on the list of classified information and its divulgence or misuse can cause damage to the interests of the Czech Republic or can be unfavourable to these interests;
q) as the originator, does not immediately declassify or change the classification level in cases when reasons will extinguish for classification of the information, the reasons for classification do not correspond to the assigned security classification or if the security classification level has been assigned without authorization;
r) does not ensure that conditions have been created as outlined in S. 33 for storing and in S. 23 par. 2 for accounting/recording, lending or transportation of classified information or classified information requiring a Special Handling Regime, or for other methods of handling;
s) operates the Information System that has not been certified by the Authority or has not been approved in writing for operation by a responsible person or by the person authorized by the responsible person;
t) operates the Communication System whose security project has not been approved by the Authority;
u) does not terminate the operation of the Information System that does not meet conditions laid down in the certification report or does not terminate the operation of the Communication System that does not meet conditions laid down in the Communication System security project;
v) uses a device for the cryptographic protection that has not been certified by the Authority, or uses the cryptographic site for purposes other than for those it has been certified and approved for operation;
w) does not ensure that the cryptographic protection will be performed by an individual who complies with requirements laid down in S. 38 par. 2;

x) does not ensure that the cryptographic device will be operated by an individual who complies with requirements laid down in S. 40 par. 2;
y) does not ensure that the cryptographic material will be transported by an individual who complies with requirements laid down in S. 42 par. 1;
z) does not report the compromise of cryptographic material according to S. 43 par. 2;
aa) does not establish the Registry or does not inform the Authority of changes in the Registry according to S. 79 par. 8 f);
bb) does not carry out the inventory of classified information according to S. 69 par. 1 m) kept in the Registry or does not notify the Authority of its result;
cc) sends classified information at the security classification level TOP SECRET, SECRET or CONFIDENTIAL contrary to S. 77; or
dd) allows performance of activities of sensitive nature to the natural person who is not holder of the valid Certificate or PSC; or
ee) does not inform, as contracting autority of a public contract or public contracting autority in concession procedure, the Authority of the fact according to S. 69 par. 1 r).

(2) The following fine will be imposed for administrative infractions up to

a) 300,000 CZK in case of an administrative infraction according to paragraph 1 a), b), c), d), e), f) or g);
b) 500,000 CZK in case of an administrative infraction according to paragraph 1 h), i), j), k), l, m, n or o);
c) 1,000,000 CZK in case of an administrative infraction according to paragraph 1 p), q), r), s), t), u), v), w), x), y), z), aa), bb), cc), dd) or ee).

403.
Section 154

(1) The facility with access to classified information commits an administrative infraction if it

a) does not hand over or forward classified information according to S. 56 par. 2;
b) does not update the facility security documents according to S. 98;
c) provides classified information at the security classification level RESTRICTED to a foreign partner contrary to S. 73 b);
d) provides classified information at security classification levels TOP SECRET, SECRET or CONFIDENTIAL to a foreign partner contrary to S. 73 a); or
e) leaves the territory of the Czech Republic with the certified cryptographic device without permission of the Authority;
f) does not send to the Authority without delay copy of the Statement of Facility according to S. 15a par. 2; or the Statement of Facility according to S. 15a par. 3; or
g) does not inform the Authority or provider of restricted information of termination of the Statement of Facility according to S. 15a par. 6.

(2) A fine will be imposed for administrative infractions up to

a) 1,000,000 CZK in case of an administrative infraction according to paragraph 1 a), b) or c;
b) 5,000,000 CZK in case of an administrative infraction according to paragraph 1d) or e);
c) 2,000,000 CZK in case of an administrative infraction according to paragraph 1f) or g).

404.
405. **Section 155**

(1) The facility that is a holder of the FSC commits an administrative infraction if

a) does not forward, according to S. 68 a), the FSC, validity of which was terminated;
b) does not report, according to S. 68 b), the loss or theft of the FSC;
c) does not report, according to S. 68 c), any change to the data as stipulated by S. 97 a), b) or p) and by S. 98 c);
d) does not report, according to S. 68 d), any change to the data in the facility application;
e) as a holder of the FSC for a foreign power, does not hand over, according to S. 57 par. 8, the invalid FSC for a foreign power;
f) as a holder of a FSC for a foreign power, does not report, according to S. 68 b), the loss or theft of a FSC for a foreign power; or
g) does not secure the protection of classified information, upon termination of validity of the FSC as outlined in S. 56 par. 2.

(2) A fine will be imposed for administrative infractions up to

a) 50,000 CZK in case of an administrative infraction according to paragraph 1 a), b), c), d), e) or f);
b) 100,000 CZK in case of an administrative infraction according to paragraph 1 g).

Section 155a

(1) The facility commits an administrative infraction if

a) makes performance of sensible activities possible to natural person who is not a holder of the valid Certificate of PSC;
b) manages to secure its access to classified information classified at the security classification level RESTRICTED without meeting conditons according to S. 15 a), or access on the basis of Statement of Facility for which conditions according to S. 15a par. 1 have not been established;
c) manages to secure its access to classified information classified at security classification levels CONFIDENTIAL or above without meeting conditions according to S. 15 b).

(2) A fine will be imposed for administrative infractions up to

a) 500,000 CZK in case of an administrative infraction according to paragraph 1 b);

b) 1,000,000 CZK in case of an administrative infraction according to paragraph 1 a) or c).

Section 156

Common provisions

(1) A legal person will not be liable for an administrative delict if it proves that it has made every reasonable effort to prevent the breach of legal obligations.

(2) The liability of the legal person for an administrative infraction shall extinguish if the Authority did not initiate proceedings against the administrative infraction within 1 year from the date on which it has become aware of this, but within 3 years at the latest from the date when the administrative infraction has been committed.

(3) The seriousness of an administration infraction shall be taken into account in determining the rate of the fine, in particular the mode of its committing and its consequences, as well as circumstances of its committing.

(4) Provisions of this Act regulating the liability of the legal person shall be applied for assessment of liability for actions in the area of protection of classified information at the time of pursuing business of a natural person or in direct relation to this business, as well as for an administrative proceedings to deal with the breach of obligations of the natural person pursuing business in the area of protection of classified information.

(5) In case of administrative proceedings to deal with the breach of obligation of the natural person in the area of protection of classified information that did not occur during his/her business activities or in direct relation to this business, the provisions of the act to make provisions for the administrative infractions shall be applied.

(6) Administrative delicts according to this Act shall be heard by the Authority.

406.

(7) Fines shall be collected by the Authority. The proceeds from fines shall be for the state budget revenue.

(8) Fines shall be due within 30 days of the date the decision on its imposition takes legal effect.

PART NINE

407. TRANSITIONAL AND FINAL PROVISIONS

408.

409. **Section 157**

410.

411. **Transitional provisions**

412.

(1) Classified information according to existing legal regulations shall be considered to be classified information according to this Act. If classified information or state and official secrets are mentioned in the existing legal regulations these shall mean classified information according to this Act.

(2) The security classification level established according to existing legal regulations shall be considered to be security classification level established according to this Act.

(3) The security classification levels of classified documents originated before 31st December 1992 shall be cancelled as from the 1st January 2008, unless otherwise specified in particular cases by the responsible person until 31st December 2007.

(4) Written records of designation according to existing legal regulations shall be considered to be the briefing according to this Act.

(5) A security clearance certifying that the person concerned meets conditions prescribed for its issuance, which has been granted according to existing legal regulations, shall be considered to be the PSC according to this Act until expiration of its validity indicated therein.

(6) A certificate of the security eligibility of the natural person that has been issued according to existing legal regulations shall be considered to be the certificate of the security eligibility of a natural person according to this Act, including the period of its validity.

(7) The notice of fulfilment of conditions for the purposes of designation of the individual concerned for the security classification level RESTRICTED that has been issued according to existing legal regulations shall be considered to be verification of fulfilment of

413. conditions of legal capacity, age and integrity for the period of 6 months from the effective date of this Act, required for giving access to a natural person to classified information at the security classification level RESTRICTED according to this Act, provided that the responsible person or classified information provider takes steps to brief the natural person concerned within 1 month from the effective date of this Act.

(8) Approval to designation of the person concerned without conducting prior security clearance procedure, which has been given according to existing legal regulations, shall be considered to be the approval for access to classified information on a one-time basis for a period of 6 months from the effective date of this Act for the classification level to which he/she is to be issued with the security clearance.

(9) The natural person who had been authorized to have access to classified information according to existing legal regulations before the effective date of this Act only on the basis of the briefing and who had not been a holder of the valid security clearance, may be authorized to have access to classified information from the effective date of this Act only if he/she is a holder of a valid PSC. This requirement does not apply in case of persons who are authorized to have access to classified information according to this Act without a valid

PSC and without a briefing.

(10) The certificate confirming to a foreign power that the person concerned has been issued with a security clearance or that the organization has been issued with a confirmation, which was issued according to existing legal regulations, shall be considered to be the PSC for the foreign power or the FSC for the foreign power until expiration of its validity indicated therein, confirming to the foreign power that the security clearance procedure has been conducted in case of a natural person or facility and that the natural person is a holder of a PSC or the facility is a holder of a FSC for the given classification level, and in case of the FSC also the forms in which classified information can be found.

(11) The confirmation that the facility meets conditions determined for its issuance, which has been issued according to existing legal regulations, shall be considered to be the FSC according to this Act until expiration of its validity indicated therein.

(12) The consent to exchange classified information between the organization and the foreign partner that has been given according to existing legal regulation shall be considered to be the permission to exchange classified information between the organization and foreign partner outside the territory of the Czech Republic according to this Act.

(13) The specialist competence certificate of a cryptographic protection officer that has been issued according to existing legal regulations shall be considered to be the specialist competence certificate of a cryptographic protection officer according to this Act until expiration of its validity indicated therein.

(14) The certificate of technical means used for the protection of classified information that has been issued according to existing legal regulations shall be considered to be the technical means certificate according to this Act until expiration of its validity indicated therein.

(15) The certificate of the Information System used for handling classified information that has been issued according to existing legal regulations shall be considered to be the Information System certificate according to this Act until expiration of its validity indicated therein.

(16) The certificate of the cryptographic device used for protection of classified information that has been issued according to existing legal regulations shall be considered to be the cryptographic device certificate according to this Act until expiration of its validity indicated therein.

(17) The classified security standard that has been issued according to existing legal regulations shall be considered to be the security standard according to this Act.

(18) The security clearance procedure initiated before the effective date of this Act will be completed in accordance with existing legal regulations. The time-limit to perform the comparable security clearance procedure according to this Act shall apply to its completion, with the understanding that the time begins to run from the effective date of this Act.

(19) The verification of the security eligibility initiated before the effective date of this Act will be completed according to existing legal regulations. The time-limit to perform the

verification according to this Act shall apply to its completion, with the understanding that the time begins to run from the effective date of this Act.

(20) The process of technical means certification, Information System certification or cryptographic device certification initiated before the effective date of this Act will be completed in accordance with this Act.

(21) A complaint lodged against the non-issuance of the security clearance, confirmation or the Certificate before the effective date of this Act shall be handled according to existing legal regulations.

(22) An application for remedial measure lodged according to existing legal regulations to the Collegium in the area of protection of classified information, which had not been decided before the effective date of this Act, will not be disposed of by the Collegium any more. In this case the Collegium will return all files to the submitting body within 5 working days from the effective date of this Act. This body shall instruct the participant in the Procedure in writing of the possibility to bring an action against the decision of the director of the Authority; in these cases the time-limit for bringing the action shall run again from the date of the service of the written instruction.

(23) An action may be brought according to this Act against the decision to dismiss the complaint issued according to existing legal regulations after the effective date of this Act.

(24) The proceedings to impose a fine initiated before the effective date of this Act will be completed according to existing legal regulations.

(25) The Communication System that has been operated before the effective date of this Act may be operated until such time as its security project has been approved, but not for the period exceeding 12 months from the effective date of this Act, provided that the responsible person of the body requests, in writing, approval of its security project within 3 months from the effective date of this Act.

(26) The site, on which the activities associated with the cryptographic protection were performed before the effective date of this Act, may be used for performance of cryptographic protection until such time that it has been approved for operation by the authorized representative, but not for the period exceeding 12 months from the effective date of this Act, and if the site is subject to certification, provided that the State body or facility request in writing to perform certification within 3 months from the effective date of this Act.

(27) The shielded chamber that has been used by the Ministry of Foreign Affairs at the Embassy of the Czech Republic for the protection of classified information before the effective date of this Act may be used by this Ministry for the protection of classified information until such time that it has been certified, but not for the period exceeding 24 months from the effective date of this Act, provided that the Ministry of Foreign Affairs requests in writing its certification within 3 months from the effective date of this Act.

(28) Conducting security investigation on a natural person, or an organization, technical means certification, Information System certification, cryptographic device certification, verification of the security eligibility of the natural person, issuance of the certificate confirming to a foreign power that the person concerned has been issued with a

security clearance or the organization with the confirmation, and issuance of the consent to exchange classified information between the organization and a foreign partner shall be governed by existing legal regulations only if the application has been consigned to the post or otherwise delivered or consigned no later than 45 days prior to the effective date of this Act.

Section 158

Delegating provisions

The Authority shall issue the regulation to implement S. 7 par. 3, S. 9 par. 8, S. 15a par. 7, S. 23 par. 2, S. 33, S. 34 par. 6, S. 35 par. 6, S. 36 par. 4, S. 44, 53 a 64, S. 75a par. 4, S. 79 par. 8, S. 85 par. 5 a S. 135

Section 159

Heading deleted

The Rules of Administrative Procedure relate only to the procedure according to Part two Chapter IX, save as otherwise provided, to the procedure according to S. 116 and to the procedure according to Part eight.

Section 160

Repealing clause

The following shall be hereby repealed:

1. Act N. 164/1999 Coll., to alter Act N. 148/1998 Coll., on Protection of Classified Information and on Amendments to Relevant Legislation.

2. Act N. 363/2000 Coll., to alter Act N. 148/1998 Coll., on Protection of Classified Information and on Amendments to Relevant Legislation, as amended.

3. Act N. 386/2004 Coll., to alter Act N. 148/1998 Coll., on Protection of Classified Information and on Amendments to Relevant Legislation, as amended.

4. Decree of the Government N. 340/2002 Coll., to lay down the list of some sensitive activities.

5. Decree of the Government N. 385/2003 Coll., to lay down the sensitive activity for the Castle Guard.

6. Decree of the Government N. 31/2005 Coll., to lay down the list of some sensitive activities for civil aviation, as amended by the Decree of the Government N. 212/2005 Coll.

7. Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information.

8. Decree of the Government N. 89/1999 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information.

9. Decree of the Government N. 152/1999 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended by the Decree of the Government N. 89/1999 Coll.

10. Decree of the Government N. 17/2001 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.

11. Decree of the Government N. 275/2001 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.

12. Decree of the Government N. 403/2001 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.

13. Decree of the Government N. 549/2002 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.

14. Decree of the Government N. 631/2004 Coll., to alter the Decree of the Government N. 246/1998 Coll., to lay down the lists of classified information, as amended.

15. Regulation N. 137/2003 Coll., regulating details of setting and marking of the security classification level and of providing the administrative security.

16. Regulation N. 245/1998 Coll., to make provisions for personal eligibility and formats of forms used in the area of personal security.

17. Regulation N. 397/2000 Coll., to alter the Regulation N. 245/1998 Coll., to make provisions for personal eligibility and formats of forms used in the area of personal security.

18. Regulation N. 263/1998 Coll., to lay down the method and procedures of verification of the security eligibility of the organization.

19. Regulation N. 12/1999 Coll., to provide for the technical security of classified information and to make provisions for certification of technical means.

20. Regulation N. 337/1999 Coll., to alter the Regulation N. 12/1999 Coll., to provide for the technical security of classified information and to make provisions for certification of technical means.

21. Regulation N. 56/1999 Coll., to provide for the security of Information Systems handling classified information, to make provisions for carrying out their certification and for elements of the certificate.

22. Regulation N. 339/1999 Coll., to make provisions for physical security.

23. Regulation N. 136/2001 Coll., to provide for the cryptographic protection of classified information, to make provisions for carrying out certification of cryptographic devices and for elements of the certificate.

24. Regulation N. 348/2002 Coll., to make provisions for security eligibility of natural persons.

431.
432. **Section 161**
433.
434. **Coming into force**
435.
436. This Act comes into force on 1 January, 2006.

Zaorálek v. r.

Klaus v. r.

Paroubek v. r.

Selected provisions of amendments

Art. II of the Act N. 255/2011 Coll.

Transitional provisions

1. Time-limits for completion of the procedure according to existing legal regulations shall apply to Procedures for granting the PSC, FSC or the Certificate that have not been completed upon a final and conclusive judgment before the effective date of this Act, if this is not the case according to the point 2; otherwise the procedure shall be completed according to Act N. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended with effect from the effective date of this Act.

437. 2. The procedure for granting the facility security clearance for access to classified information at the security classification level RESTRICTED and the procedure concerning termination of validity of the FSC for access to classified information at the security classification level RESTRICTED, which have not been completed by final and conclusive judgment before the effective date of this Act shall be terminated on the effective date of this Act.
438.
439. 3. Validity of the Notice issued by the Authority according to existing legal regulation will terminate on the first day of the third calendar month following the effective date of this Act.
440.
441. 4. Proceedings to impose a fine for administrative infraction or other administrative delict, which have not been completed upon a final and conclusive judgment before the effective date of this Act will be completed according to existing legal regulations.

5. Facility security clearance for the security classification level RESTRICTED that has been issued according to existing legal regulations shall be considered within 3 months from the effective date of this Act to be the the Statement of Facility according to the Act N. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended with effect from the effective date of this Act.

Art. LXXXII of the Act N. 458/2011 Coll.

442. Transitional provision. As economically unstable according to the provision of S. 17 par. 2 of the Act N. 412/2005 Coll., as amended, can also be considered the facility within the period of 2 years from the effective date of this Act, which is deficient towards the appropriate body of social welfare or appropriate health insurance company in due social welfare insurance payment, in state employment policy allowance or public health insurance payments for the period preceding the effective date of this Act.