COLLECTIONS OF LAWS

OF THE SLOVAK REPUBLIC

2004

215

ACT

of 11 March 2004

on Classified Information Protection and Amendment and Supplementing some Acts

The National Council of the Slovak Republic has resolved on the following Act:

Article I

PART I

GENERAL PROVISIONS

Article 1
Scope of the Act

(1) This Act regulates the conditions for classified information protection, the rights and obligations of corporate entities and individuals pertaining thereto, the jurisdiction of the National Security Authority (hereinafter referred to as "the Authority") and the jurisdiction of other state authorities in relation to classified information, and the liability for violation of the obligations stipulated by this Act.

(3) This Act does not apply to the protection of secrets pursuant to specific legal regulation.[1a])

Article 2
Basic Terms

For the purposes of this Act:

a) classified information shall be any information or object specified by the originator of the classified information, which must, in the interests of the Slovak Republic, remain protected from disclosure, damage, unauthorized duplication, destruction, loss or theft (hereinafter referred to as "unauthorized handling") and which may occur only in fields stipulated by the Government of the Slovak Republic through its regulation,

b) information shall be

[1a]) E.g. Article 17 of Commercial Code, Article 91 of Act No. 483/2001 Coll. on Banks and on Amendment and Supplementing some Acts, as amended, Article 23, 23a and 23b of Act of the Slovak National Council No. 511/1992 Coll. on Tax and Fees Administration and on Changes in the System of Territorial Financial Bodies, as amended.

1. the content of documents, sketches, drawings, maps, photographs, graphs or other records,

2. the content of verbal statements,

3. the content of electric, electromagnetic, electronic or other physical transport media,

c) object shall be

1. a physical carrier with recorded information,

2. a product,

3. equipment,

4. real estate,

d) detriment shall be damage, or a threat thereof, pertaining to the interests of the Slovak Republic or interests whose protection the Slovak Republic has committed to, the consequences of which could not be eliminated or could only be mitigated by a measure subsequently undertaken; depending on the significance of the interest and the severity of the detriment, the latter shall be categorized as extremely serious detriment, serious detriment, simple detriment and prejudicial to the interests of the Slovak Republic,

e) originator of classified information shall be a corporate entity or individual authorized to decide that an information pursuant to subparagraph b) or an object pursuant to subparagraph c) is classified information, to determine the classification level and to decide in matters of amendment or revocation of the security classification level,

f) authorized person shall be a corporate entity or individual designated for acquaintance with classified information or whose authorization for acquaintance with classified information stems from the law,

g) unauthorized person shall be an individual not authorized for acquaintance with classified information, or not authorized for acquaintance with classified information beyond the designated scope pertaining to that person,

h) foreign power shall be a foreign state, authorities of a foreign state or organizations used by a foreign state in controlling or carrying out its powers and activities; foreign powers are also supranational organizations, international organizations and associations of states,

i) technical device shall be an equipment, or a system designed to create, process, transfer, store and protect classified information,

j) certification activity shall be an activity used to verify and certify, whether a technical device, a means for protecting information by encryption, mechanical prevention device or technical safeguarding device is fit to protect classified information,

k) authorization shall be an appointment of the state authority or corporate entity to carry out an activity in certification,

l) certifying authority shall be the carrying out of functions pertaining to the issuance and verification of digital certificates of public keys used in asymmetrical encryption systems,

m) digital certificate shall be an electronic confirmation of the assignment of a public signature key to a specific subject, thereby validating their identity,

n) public signature key shall be a cryptographic key used in validating an electronic signature,

o) information protection encryption system shall be a set of devices for encryption protection of information together with the whole infrastructure for generating, distributing and destruction of encryption materials past their validity,

p) information protection encryption device shall be equipment designed for protection of information by encryption, and encryption materials,

r) building shall be a construction or otherwise delimited premises with protected areas situated inside,

s) protected areas shall be a construction or otherwise delimited premises within a building, intended for storage and handling of classified information, corresponding to the respective security classification level,

t) mechanical prevention device is an equipment or a system for preventing unauthorized persons from gaining access,

u) technical safeguarding device shall be an equipment or a system providing information on the state of the breaching of a building or protected area.

Article 3

Security Classification Levels

(1) Classified information shall be categorized according to the security classification level into

a) Top secret,

b) Secret,

c) Confidential,

d) Restricted.

(2) The security classification level shall be marked with the words "Prísne tajné"-[Top Secret], "Tajné"-[Secret], "Dôverné"-[Confidential], "Vyhradené"-[Restricted], or with the acronyms "PT", "T", "D" and "V".

(3) Security classification level Top Secret shall be used to mark classified information whose unauthorized handling could have the consequence of seriously endangering the constitutionality, sovereignty and territorial integrity of the state, or could cause irreparable and serious damage in defense, security, economic interests, foreign policy or international relationships, and thus could cause extremely serious damage to the interests of the Slovak Republic.

(4) Security classification level Secret shall be used to mark classified information whose unauthorized handling could have the consequence of endangering the foreign policy standing, defense, security and interests of the state in the international and economic field, and thus could cause serious damage to the interests of the Slovak Republic.

(5) Security classification level Confidential shall be used to mark classified information whose unauthorized handling could have the consequence of damaging the interests of the state, public interests or legally protected interests of a body of the state administration, and thus cause simple damage to the interests of the Slovak Republic.

(6) Security classification level Restricted shall be used to mark classified information whose unauthorized handling could damage the legally protected interests of a corporate entity or an individual and which thus could be inconvenient to the interests of the Slovak Republic.

Article 4
Prohibition of Classification of some Information

(1) Classified information cannot be information on

a) unlawful or incorrect procedure or unlawful decision of public agents and public authorities,

b) criminal activity of public agents,[2])

c) uneconomic, inefficient and ineffective handling of public funds,

d) serious jeopardy or damage to the environment, life and health,

e) salary, material provision and material advantages of public agents.

(2) If information contains, besides materials pursuant to paragraph 1, also other partial information subject to security classification, the originator of the classified information shall take measures to restrain causing damage to the protected interests.

PART II

CLASSIFIED INFORMATION PROTECTION

TITLE I

BASIC PROVISIONS

Article 5
Classified Information Protection Policy

(1) Classified Information Protection Policy of the Slovak Republic is a set of aims, restrictions, requirements, rules and procedures that determine the manner and development of the classified information protection. The Classified Information Protection Policy of the Slovak Republic shall be approved by the Government of the Slovak Republic at the proposal of the Authority's Director.

(2) Ministries and other central bodies of state administration of the Slovak Republic[3])(hereinafter referred to as "central state administration body") adapt the Classified Information Protection Policy to their conditions in accordance with the Classified Information Protection Policy of the Slovak Republic.

Article 6
Classified Information Protection

(1) Classified information shall be protected from unauthorized persons and foreign powers in a manner stipulated pursuant to this Act, in regulation issued for its carrying out, and in further specific legal regulation.[4])

(2) Classified information protection is creation of conditions for personnel security, administrative security, encryption protection of information, physical security, building security, security of technical devices and industrial security.

(3) Information that is classified information is upon its transfer by technical devices to be protected by information encryption devices.

---

[2]) Article 89(9) of Criminal Code, as amended.

[3]) Act No. 575/2001 Coll. on the Organisation of Government Activity and onOrganisation of the Central State Administration, as amended.

[4]) E. g., Criminal Code, as amended, Criminal Proceedings Code, as amended, Article 174(1) and Article 203 of Civil Procedure Code, Article 111 and 126 of Administrative Court Proceedings Code.

(4) Personnel security is a system of measures pertaining to the selection, appointment and checking of persons authorized for acquaintance with classified information of defined scope.

(5) Administrative security is a system of measures whose objective is to ensure classified information protection at the time of their creation, receiving, recording, transfer, storage, duplication, disposal and archiving, or other handling.

(6) Physical security and building security is a system of measures ensuring classified information protection against unauthorized persons and against unauthorized handling in buildings and protected areas.

(7) Security of technical devices is a system of measures for ensuring the protection of classified information created, processed, transferred or stored in technical devices.

(8) Industrial security is a set of measures of a corporate entity or an individual performing business activities pursuant to specific legal regulation[5)](hereinafter referred to as "an entrepreneur") for the protection of classified information submitted to, or originating at such an entrepreneur.

(9) Encryption protection of information a system for securing classified information protection by cryptographic methods and by means of encryption protection of information.

(10) The Authority shall be authorized to issue generally binding legal regulation governing details of personnel security, administrative security, of physical security and building security, of security of technical devices and of industrial security.

Article 7

Amendment and Revocation of Security Classification Level

(1) If the need to protect information or an object containing classified information at a certain security classification level has expired, the originator of the classified information shall decide on an amendment or revocation of the security classification level. If a stipulated period for the security classification level of information or an object containing classified information has expired, the originator of the classified information shall decide on an amendment or revocation of the security classification level.

(2) If a corporate entity, in which the security classification level has been designated, ceases to exist without a legal successor, or if the originator of the classified information is not known, the head of the state authority within whose scope the classified information falls shall decide on an amendment or revocation of the security classification level.

(3) The archiving and protection of classified information that, pursuant to a specific legal regulation,[6)] has permanent documentary value, shall be ensured by the central body of the state administration within whose scope the classified information falls.

Article 8

Duties of the Head

(1) The responsibility for classified information protection in a state administration body lies with the statutory body, in a municipality with its mayor, in a higher territorial unit with its chairperson, and in any other corporate entity with its statutory body (hereinafter referred to as "the head"); in cases where the statutory body is a collective body, the head for the purposes of this Act shall be the holder of a written authorization issued by the collective body to one of its members.

---

5) E, g, Article 2 of Commercial Code, as amended.
6) Act No. 395/2002 Coll. on Archives and Registres and on Amendment of some Acts.

(2) The head shall in particular

a) determine the basic scope of classified information, and unless they determine otherwise, decide on the period of, amendment to and revocation of the security classification level pursuant to Article 7(1),

b) determine and be responsible for the classified information protection policy and create conditions for its implementation,

c) ensure inspection of classified information within own jurisdiction and at the entrepreneurs to whom classified information has been transferred by the head,

d) determine the positions whose carrying out allows authorized persons to get acquainted with classified information,

e) provide for carrying out of 1st degree security clearance,

f) request the Authority to execute 2nd through4th degree security clearance of persons proposed to be designated for acquaintance with classified information at the security classification levels Confidential, Secret or Top Secret,

g) designate the person proposed to get acquainted with classified information (hereinafter referred to as "the nominee") and revoke such a designation, determine the scope and need to know for persons to get acquainted with classified information, and ensure their acquaintance with the rights and obligations pursuant to this Act and regulation issued for its implementation,

h) ensure the briefing of persons who are to get acquainted with classified information of the security classification level Restricted, that have been transferred to the Slovak Republic by a foreign power; the briefing is carried out pursuant toto the requirements of the foreign power,

i) to notify the Authority in advance of the dissolution, fusion, merger, abolishment or splitting up of a state body or corporate entity at which classified information is stored,

j) maintain registers and lists of authorized persons and of persons whose authorization has expired,

k) notify the Authority on changes in the scope of acquaintance with classified information that has occurred pertaining to an authorized person, changes in the name and surname, marital status, address of permanent residence and citizenship of the authorized person, as well as on other facts reliably learnt and relevant for the inception of the authorization pursuant to Article 10(1),

l) notify the Authority without undue delay on any unauthorized handling of classified information and attempted violation of classified information protection,

m) inform the Authority of commencing research, development, design or production, if classified information at the security classification levels Top Secret, Secret or Confidential is involved,

n) notify the Authority in advance on the preparation and conclusion of an international agreement or commercial contract with a foreign entity or with the participation of a foreign entity, if classified information is involved,

o) perform other measures pertaining to classified information protection stemming from this Act or an international agreement,

p) prepare annual reports on inspections of the classified information protection, specifying in particular data on the number of checks performed, shortcomings identified and remedial measures taken; submitting a report for the previous calendar year by the end of February to the Authority,

r) send to the Authority by the end of February, in electronic form or in writing a list of all classified documents marked with security classification level Top Secret and Secret, that were filed in the protocols of documents of the respective security classification levels in the previous calendar year; the list shall specify the number of the classified document, number of its pages and its originator; the matter to which the classified information pertains shall not be stated in the list.

(3) Should a person be about to become the head and be designated for acquaintance with classified information, the request for carrying out a security clearance pursuant to paragraph 2f) shall be submitted by the person appointing, electing, or otherwise assigning to the position of the head. Article 35(1) applies to carrying out security clearance of a mayor of a municipality or chairman of a higher territorial unit.

Article 9

Special Workplace

(1) The head may, for the fulfillment of tasks stemming from this Act and from the regulation for its implementation, establish a special workplace, or appoint an employee in writing (hereinafter referred to as "the security employee"), to carry out these tasks in the scope defined by the head. If the quantity of tasks to be fulfilled or the complexity of the organizational structure requires so, the head may establish several special workplaces or appoint in writing several security employees. Prerequisite to carry out the position of security employee and employee of the special workplace is the holding of a valid personnel security clearance certificate, issued by the Authority, for acquaintance with classified information (hereinafter referred to as "the certificate") and confirmation, issued by the Authority, of having passed the security employee examination.

(2) The Authority shall issue generally binding legal regulation stipulating the particulars of the security employee examination.

TITLE II

AUTHORIZATION FOR ACQUAINTANCE WITH CLASSIFIED INFORMATION

Article 10

Prerequisites for the Inception of an Authorization

(1) Unless stipulated otherwise in this Act, the authorization for acquaintance with classified information for the security classification levels Top Secret, Secret, Confidential or Restricted shall be contingent upon the nominee

a) being a citizen of the Slovak Republic,

b) having full legal capacity,

c) having reached the specified age,

d) agreeing to get acquainted with classified information and to undergo security clearance,

e) being of integrity,

f) guaranteeing through their conduct that they shall ensure classified information protection,

g) being reliable as regards security,

h) having a valid certificate, issued by the Authority, according to which they may get acquainted with classified information of the security classification level Top Secret, Secret or Confidential,

i) having been accordingly designated,

j) having signed the non-disclosure declaration.

(2) The nominee shall continue to fulfil the conditions for the inception of the authorization pursuant to paragraph 1 throughout the entire period of validity of the certificate pursuant to Article 28, or the designation pursuant to Article 31.

(3) A nominee who is to get acquainted with classified information at the Restricted security classification level, shall fulfil the conditions for the inception of the authorization pursuant to paragraph 1 except for subparagraph h), and shall be designated pursuant to Article 31, paragraphs 1 and 2.

Article 11

Age of the Nominee

(1) The age limit for a nominee for the security classification level

a) Top Secret shall be at least reaching 21 years,

b) Secret, Confidential and Restricted shall be at least reaching 18 years.

(2) The provision of paragraph 1a) does not apply to nominees serving in the armed forces, in the service relationship of an officer of the armed security corps, an officer of the armed corps or officer of the Slovak Information Service (hereinafter referred to as "service relationship").

(3) The provision of paragraph 1b) does not apply to students of secondary military schools.

Article 12

Integrity of the Nominee

(1) For the purposes of this Act persons shall not be considered of integrity if they have been lawfully convicted for an intentional criminal offence, unless they are deemed not having been convicted.

(2) Even if a nominee is deemed not having been convicted, for the purposes of 2nd, 3rd, and 4thdegree security clearance they shall not be considered persons of integrity if having been lawfully convicted

a) for a particularly serious felony, or

b) for an intentional criminal offence of endangering classified information or for the criminal offence of endangering Confidential or Restricted classified information.

(3) In 1st degree security clearance the nominees shall prove their integrity through an extract from the Criminal Records Register.[10)] In 2nd, 3rd, and 4thdegree security clearance integrity is proven by an extended extract of the Criminal Records Register.[10)] For the purposes of proving their integrity in the 1st , 2nd, 3rd, and 4thdegree security clearance the individuals shall provide all necessary data for requesting the respective extracts from the Criminal Records Register.[10a)] The data according to the third sentence shall be sent by the head without delay in electronic form via electronic communication to the General Prosecutor's Office of the Slovak Republic to issue the respective extract from the Criminal Records Register; the above-mentioned does not apply to the Slovak Information Service, if it could endanger the fulfillment of the tasks pursuant to this Act or specific legal regulation.[10b)]

[10)] Act No. 330/2007 Coll. on Criminal Records Register and on Amendment and Supplementing some Acts.

[10a)] Article 10(4) of Act No. 330/2007 Coll. on Criminal Records Register and on Amendment and Supplementing some Acts, as amended by Act No. 91/2016 Coll.

[10b)] Act of the National Council of the Slovak Republic No. 46/1993 Coll. on Slovak Information Service, as amended.

Article 13
Conduct of the Nominee

Persons who

(1) according to the conclusions of the medical examination are dependent on the use of alcoholic beverages or the use of other addictive substances,[11])

(2) have been repeatedly sanctioned over the last five years for an offence in classified information protection pursuant to Article 78,

shall not be deemed persons able, through their conduct, to guarantee classified information protection.

Article 14
Security Reliability of a Nominee

(1) Persons shall not be deemed reliable as regards security, if they have provided false data in their personal questionnaire, in their security questionnaire, at a security interview, or who was assigned to and actively carried out activity in the established structures of the former State Security pursuant to Annex No. 1 or of the former Intelligence Directorate of the Czechoslovak People's Army Headquarters until 31 December 1989 – with the exception of persons who carried out in these structures only an ancillary service or safeguarding position – or knowingly collaborated with these structures, or in the case of whom a security risk has been identified.

(2) A security risk shall be deemed to be

a) an activity performed against the interests of the Slovak Republic in the field of defense of the state, security of the state, international contacts, economic interests of the state, activity of a state body, or against interests that the Slovak Republic has undertaken to protect pursuant to international agreements,

b) the premeditated violation of legal regulation, with consequences potentially endangering interests of the Slovak Republic,

c) a finding that the person

1. is or has been a partner of spies, terrorists, saboteurs or of other persons having been reasonably suspected of such activities in the past,

2. is or has been a member or supporter of any organization striving by violent, subversive or other illegal means to remove the democratic social order,

3. is under provable duress in consequence of own financial situation,

4. is provably dependent on the consumption of alcoholic drinks or other addictive substances,

5. is or has been involved in any form of sexual conduct leading to blackmail or to constraint,

6. has proved dishonesty, untrustworthiness pertaining to classified information protection, through their conduct or expression,

7. has seriously or repeatedly violated security regulations by trying to penetrate communication and information systems without authorization,

8. suffers or has suffered any illness or mental or emotional condition that could cause substantial disorders in their reasoning and behavior,

---

[11]) Article 89(11) of Criminal Code.

9. is under provable pressure from relatives or close friends who are open to exploitation by foreign intelligence and information services, terrorist groups, illegal organization, risk groups or other similar individuals,

10. accepts unjustified payments, gifts or other benefits, or misuses own status and position in pursuit of the acquisition of unjustified benefits,

11. owns property whose value is not commensurate with the declared income and the lawful origin of which is unable or unwilling to prove,

12. has completed study, a course or training of a security nature at the KGB University of Felix Edmundovich Dzerzhinsky in the former Union of Soviet Socialist Republics.

Article 15

Security Clearance of a Nominee

(1) Security clearance is carried out in order to ascertain, whether the nominee meets the requirements stipulated in Article 10(1) for acquaintance with classified information.

(2) According to the security classification level the following shall be carried out

a) 1st degree security clearance for security classification level Restricted,

b) 2nd degree security clearance for security classification level Confidential,

c) 3rd degree security clearance for security classification level Secret,

d) 4th degree security clearance for security classification level Top Secret.

Article 16

Materials for Security Clearance

(1) Materials for security clearance (hereinafter referred to as "background material") shall, unless stipulated otherwise pursuant to this Act, be

a) materials submitted by the nominee, namely

1. completed personal questionnaire pursuant to Annex No. 2,

2. curriculum vitae,

3. an extract from the Criminal Register Records not older than three months in the case of 1stdegree security clearance unless it's impossible to use data from public administration information system,

4. written consent to the authorization to get acquainted with classified information and to undergo security clearance,

5. completed security questionnaire pursuant to Annex No. 3 for security clearance of the 2nd, 3rd and 4th degrees,

b) information from the records of the Police Force, Slovak Information Service and Military Intelligence on the security reliability of the nominee,

c) information requested from other state bodies and other corporate entities on the security reliability of the nominee,

d) information on security reliability of the nominee, based on security checks carried out at the place of residence by the Police Force, Slovak Information Service or Military Intelligence,

e) information requested from the municipality in which the nominee is permanently or temporarily resident,

f) information from security checks carried out by the Police Force, Slovak Information Service or Military Intelligence on the security environment in which the nominee lives and associates and on the potential occurrence of security risks.

(2) The nominee shall submit the background material pursuant to paragraph 1a) to their head; the nominee in their up-to-date personal questionnaire, curriculum vitae and security questionnaire is obliged to state complete and truthful data. In the case of performing a 2nd, 3rd or 4th degree security clearance the nominee shall submit the security questionnaire to their head in a sealed envelope so as to prevent the head from acquainting with the contents.

(3) The head shall submit the background materials submitted by the nominee pursuant to paragraph 1a), as necessary for the performance of 2nd, 3rd and 4th degree security clearances, to the body competent to carry out the security clearance, and shall attach to them an evaluation of the background materials pursuant to paragraph 1a), subparagraphs 1 through 4.

(4) An application for carrying out of a security clearance of a state citizen of the Slovak Republic who is or is to be an employee of a body of the European Union may be submitted by the respective body of the Council of the European Union or the European Commission. The nominee shall submit the background materials pursuant to paragraph 1a) to the Authority. The provisions of Article 24(3) and Article 26(5) apply accordingly.

(5) Carrying out of a security clearance of a nominee may be requested also by an individual, a commission or other body, if stipulated so in specific legal regulation.[11])

(6) The nominee shall be authorized to provide the personal data required in accordance with Annex No. 3.[12])

Article 17

Carrying out of Security Clearances

Security clearances, except for those pursuant to Article 18, shall be carried out by

a) the head, regarding 1st degree security clearance,

b) the Authority, regarding 2nd, 3rd or 4th degree security clearance.

Article 18

(1) Slovak Information Service shall carry out security clearances of all degrees, if the nominee is an officer, an employee or applicant for admission into employment or a similar labor relationship to the Slovak Information Service, including a service relationship.

(2) Military Intelligence shall carry out security clearances of all degrees, if the nominee in the relationship to the Military Intelligence is its officer, an employee or applicant for admission into employment or a similar labor relationship, including a service relationship.

(3) Military Intelligence shall carry out also security clearances of 2nd, 3rd and 4th degrees, if the nominee is an employee of, or is in a similar labor relationship to, including service relationship to, the Ministry of Defense of the Slovak Republic (hereinafter referred to as the "Ministry of Defense"), or to organizations established or founded by the Ministry of Defense. It shall submit to the Authority the background materials pursuant to Article 16(1), together with the evaluation and proposal how to complete the security clearance pursuant to Article 26. Disputes regarding how to complete a security clearance between the Military Intelligence and the Authority shall be decided by the authority competent to decide on an appeal pursuant to Article 30(3).

---

11) E. g. Act No. 335/1991 Coll. on Courts and Judges, as amended, Act No. 385/2000 Coll. on Judges and Associate Judges as amended, Act No. 153/2001 Coll. on Public Prosecution, as amended, Act No. 154/2001 Coll. on Prosecuting Counsels and LegalReversioners of the Public Prosecution, as amended.

12) Article 7 (5) and Article 9 (1)a) of Act No. 428/2002 Coll. on Personal Data Protection.

(4) Police Force shall carry out security clearances for all security degrees, if the nominee is a member of the Police Force or its employee, or is an applicant for admission into employment or into a similar labor relationship, including service relationship, and fulfills or will fulfill criminal intelligence duties.

(5) Slovak Information Service, Military Intelligence and Police Force, in carrying out security clearances pursuant to paragraphs 1 through 4 are authorized to obtain the information stipulated in Article 16(1) b) through f) by their own activity.

Article 19

While carrying out security clearances of 2nd, 3rd and 4th degree, the Authority, Slovak Information Service, Military Intelligence and Police Force shall be authorized to request the provision of information as necessary for carrying out of the security clearance and stipulated in Article 16(1)b) through f), including personal data,[13]) from other state bodies, other corporate entities and individuals; these bodies and persons shall be obliged to comply with the request within the designated period and allow insight into the background materials on the basis of which the information for the security clearance purposes was provided. Corporate entities or individuals providing information on the nominee pursuant to Article 16 paragraph 1subparagraphs(c) to f) must get additionally acquainted with the reason for which the nominee is being subject to security clearance.

Article 20

1stDegree Security Clearance

1st degree security clearance consists of an evaluation of the background materials stipulated pursuant to Article 16(1)a) items 1 through 4.

Article 21

2ndDegree Security Clearance

2nd degree security clearance consists of an evaluation of the background materials stipulated pursuant to Article 16(1)a) through c).

Article 22

3rdDegree Security Clearance

3rd degree security clearance consists of an evaluation of the background materials stipulated pursuant to Article 16(1)a) through e).

Article 23

4thDegree Security Clearance

4th degree security clearance consists of an evaluation of the background materials stipulated pursuant to Article 16(1) a) through f).

Article 24

Commencement and Ceasing of a Security Clearance

(1) 2nd, 3rd and 4th degree security clearances shall commence on the day of delivery of the request and background materials pursuant to Article 16(1) a) items 1 through 5 to the Authority.

(2) The Authority shall cease carrying out of security clearance,

a) if the nominee has revoked the written consent to undergo the security clearance,

b) the nominee at the request of the Authority pursuant to Article 27(3) failed to remove discrepancies within the designated period,

---

[13]) Act No. 122/2013 Coll. on Personal Data Protection and on Amendment ans Supplementing some Acts, as amended by Act No. 84/2014 Coll.

c) the nominee has died,

d) it lacks competence to perform it,

e) upon verifying the new facts pursuant to Article 29 fails to find reasons to revoke the validity of the certificate or

f) the nominee fails to show up to security interview upon summons; regarding the summons Article 27(4) applies accordingly.

(3) The Authority shall cease carrying out of the security clearance also upon written request of the head who requested it. In the request the head is obliged to state the reasons for ceasing the security clearance.

(4) The Authority shall interrupt the security clearance, if there is an ongoing proceeding in which an issue which might be of significance to completion of security clearance is being solved, until the completion of the proceedings.

Article 25

Security Interview

(1) A security interview shall be held with the nominee, if within the course of a security clearance, ascertained facts might be an impediment to the issuing of a certificate or represent a reason for the revocation of the certificate validity. In the course of the security interview the nominee shall have the possibility to express their opinion pertaining to as curtained facts. A written record of the security interview shall be made and signed by the parties involved. A refusal to sign shall be noted in the record, along with the reasons for the refusal and objections against the contents of the record.

(2) A security interview with a nominee pursuant to paragraph 1 shall be held by the body that carried out the security clearance, applying such methods as to avoid the violation of third-party rights and so as to not endanger any information source.

(3) Only upon request of the nominee, the security interview may include a psycho-physiological examination of truthfulness. The nominee shall be advised of this possibility.

(4) A psycho-physiological verification of truthfulness takes place whenever the statement of the nominee during the security interview is against the ascertained facts that might be an impediment for issuing of a certificate or cause for revocation of the certificate validity.

Article 26

Completion of a Security Clearance

(1) If the Authority, upon carrying out security clearance, as certains that the nominee fulfils the conditions for the inception of an authorization pursuant to Article 10(1), it shall, instead of a written decision, issue a certificate.

(2) If the Authority, upon carrying out security clearance, ascertains that the nominee does not fulfil the conditions for the inception of an authorization pursuant to Article 10(1), it shall issue a decision to that effect.

(3) The decision issued pursuant to paragraph 2 must state the provision under which the Authority decided that the nominee cannot get acquainted with classified information, the facts providing the basis for this decision, what considerations were entered into by the Authority in evaluating the evidence, and a notice informing the nominee of the possibility to lodge an appeal.

(4) The certificate pursuant to paragraph 1 and the decision pursuant to paragraph 2 shall be delivered in writing to the nominee through personal service.

(5) The outcome of the security clearance shall be notified in writing to the head who requested the security clearance to be carried out.

Article 27
Period for Decision

(1) The Authority is obliged to decide on a security clearance of

a) 2nd degree within three months from the commencement of proceedings,

b) 3rd degree within four months from the commencement of proceedings,

c) 4th degree within six months from the commencement of proceedings.

(2) State bodies and other corporate entities pursuant to Article 16(1) b) through f) are obliged to submit to the Authority information on the security reliability of a nominee pertaining to

a) 2nd degree security clearance within two months from the delivery of the request for disclosure of information,

b) 3rd degree security clearance within three months from the delivery of the request for disclosure of information,

c) 4th degree security clearance within five months from the delivery of the request for disclosure of information.

(3) If it is not possible, given the nature of the matter, to decide in the periods pursuant to paragraph 1, the Authority may extend them by maximum another three months. The Authority is obliged to notify the nominee and the head who requested carrying out of the security clearance of the period extension, along with a statement of the reasons.

(4) If a request or background materials pursuant to Article 16(1)a) items 1 through 5 have deficiencies due to which it is not possible to commence carrying out of the security clearance, the Authority shall request the nominee to remove them within a designated period; concurrently it shall advise the nominee that in the case of a failure to remove the deficiencies the security clearance shall be ceased.

(5) The Authority shall interrupt a security clearance, if the nominee has been requested to remove deficiencies pursuant to paragraph 4.

Article 28
Validity of the Certificate

(1) The validity of a certificate is five years for the security classification level Top Secret, seven years for the security classification level Secret, and ten years for the security classification level Confidential.

(2) The validity of a certificate issued on the basis of security clearance pursuant to Article 18(1), (2) and (4) shall expire on the date of termination of employment or another similar labor relationship, including the service relationship; the validity of a certificate issued pursuant to Article 18(4) shall expire also when the nominee ceases to fulfill the criminal intelligence tasks.

Article 29
Revocation of a Certificate Validity

Upon ascertaining new facts, the Authority is during the validity of a certificate obliged to verify whether a person fulfils the conditions for the inception of the authorization pursuant to Article 10(1) and in the case it ascertains the contrary, is obliged to revoke the certificate validity. The provisions of Articles 24 through 26 apply to such a revocation of a certificate validity accordingly.

Article 30

Procedure for Reviewing Decisions of the Authority

(1) A decision of the Authority pursuant to Article 26(2), Article 29, Article 50(2) and (5) and Article 60(7), except for a decision of the Slovak Intelligence Service, Military Intelligence and Police Force, may be appealed by the person the decision had been served, within 15 days from the date of delivery of the decision. An appeal shall be lodged in writing, delivered to the Authority and it shall contain the facts by which the nominee justifies cancellation of the decision. An appeal has suspensive effect.

(2) The Authority may itself decide on an appeal alone if it grants the appeal in full. If the Authority does not itself decide on the appeal alone, it shall submit it along with the opinion on the appeal lodged and other file documents pertaining to the challenged appealed decision to the body competent to decide on an appeal (hereinafter referred to as "Appellate Body"), namely within 30 days from the date when it was delivered the appeal.

(3) The disputes regarding how to complete a security clearance between the Military Intelligence and the Authority pursuant to Article 18(3), and pertaining to an appeal pursuant to paragraph 1 shall be decided by the Appellate Body, which is the Committee of the National Council of the Slovak Republic established pursuant to a specific legal regulation.[13a]) The procedure of the Appellate Body shall be stipulated by a specific legal regulation.[13a]) The legal costs pertaining to the appeal pursuant to paragraphs 1 through 3, including the costs of the court proceedings,[13a]) shall be borne by the Authority.

Article 31

Designation of the Nominee

(1) Designation of a nominee for acquaintance with classified information shall be performed by the head before commencement of such acquaintance, by determining the security classification level and the scope of classified information with which the person needs to get acquainted in the course of carrying out their position or fulfilling the tasks of their position. A component of the designation is also acquaintance of the person with obligations in the classified information protection and the potential consequences of their violation. Authorization of the nominee for acquaintance with classified information commences by signing of a record on the designation of the nominee for acquaintance with classified information and signing the non-disclosure declaration.

(2) Designation of a nominee fulfilling the conditions for the Restricted security classification level shall be carried out by the head upon evaluation of a 1st degree security clearance. If the nominee fails to fulfil any of the conditions pursuant to Article 10(1), the head shall notify them of this fact in writing.

(3) Designation of a nominee for the Top Secret, Secret or Confidential security classification levels shall be carried out by the head only upon receipt of a written notice pursuant to Article 26(5).

(4) Designation of the head pursuant to paragraph 1 shall be carried out by the person proposing, nominating, electing or otherwise appointing the head to the position.

(5) Designation of a statutory body of a corporate entity as a person to whom classified information is to be transferred, shall be carried out by the head of the state body that would transfer the classified information; designation of the head of the entrepreneur to which classified information is to be transferred, or of the head of the entrepreneur to be requested pursuant to Article 43 to create classified information, shall be carried out by the Authority.

[13a]) Constitutional Act No. 254/2006 Coll. on Establishment and Activitiy of the Commitee of the National Council of the Slovak Republic for Reviewing Decisions of the National Security Authority.

(6) Designation of the nominee for acquaintance with classified information of a higher security classification level authorizes access to classified information at lower security classification levels within the designated scope.

Article 32

(1) A record of the nominee's designation for acquaintance with classified information of a designated security classification level, and their non-disclosure declaration shall be attached to the document by which the employment or other similar labor relationship is established or changed.

(2) The head or the security employee shall send to the Authority a copy of the record of the nominee's designation for acquaintance with classified information of the Top Secret, Secret or Confidential security classification level and a copy of their non-disclosure declaration within 30 days of that person's designation.

Article 33

Security File of a Person

(1) The Authority shall maintain a security file of a person, containing the background material from the security clearance for the Top Secret, Secret and Confidential security classification levels, a record of the security interview and findings from the security clearance.

(2) The security file of a person contains also a copy of the certificate, a copy of the designation record of the person for acquaintance with classified information of the respective security classification level, a copy of the non-disclosure declaration, and other facts notified pursuant to this Act.

(3) Data from the security file of a person may be used only to fulfil tasks pursuant to this Act and for the purposes of criminal proceedings and administrative offence proceedings in the case of unauthorized classified information handling.

(4) The data contained in the security file of a person represents data subject to classified information protection and the provisions of a specific legal regulation on the protection of personal data do not apply thereto.[14])

(5) Unless stipulated otherwise below, a security file of a person is a component of the Authority's system of records pursuant to Article 42.

Article 34

Authorized Persons having Special Status

(1) The following persons are authorized persons having special status within the scope of their respective positions pursuant to this Act

a) the President of the Slovak Republic,

b) Deputy of the National Council of the Slovak Republic,

c) member of the Government of the Slovak Republic

d) judge of the Constitutional Court of the Slovak Republic,

e) the Chairman and Deputy Chairman of the Supreme Audit Authority of the Slovak Republic and

f) a judge.

(2) The persons pursuant to paragraph 1 shall become authorized persons upon being elected or appointed to their office, or after pledging allegiance, if stipulated pursuant to specific legal regulation.

(3) Unless stipulated otherwise pursuant to this Act, pursuant to a specific legal regulation[15)] or pursuant to an international agreement binding upon the Slovak Republic, a security clearance shall not be carried out on the persons stipulated pursuant to paragraph 1.

Article 35

Other Authorized Persons

(1) Chairman of a higher territorial unit and mayor of a municipality may, in the scope required for the carrying out their office, get acquainted with classified information at the Restricted security classification level without undergoing security clearance. The head or security employee of a state body that transfers the classified information, shall advise the chairman of the higher territorial unit or municipality mayor of their obligations pertaining to the classified information protection and pertaining to the potential consequences of their violation, and shall ensure their signing of a non-disclosure declaration. If a municipality mayor or chairman of a higher territorial unit is to get acquainted with classified information of the security classification level Confidential through Top Secret, they shall request the Authority to carry out a security clearance of the respective degree on them.

(2) An accused party, their attorney and other persons pursuant to specific legal regulation,[16)] a witness at risk and a witness under protection,[17)] a person acting in the interests of the authorities pursuant to specific legal regulations,[18)] a person acting on an agreement pursuant to specific legal reulation[18a)]and an agent[19)] may, upon signing the non-disclosure declaration and after being advised of their obligations pertaining to classified information protection and the potential consequences of their violation, get acquainted with classified information in the scope necessary without fulfilling the conditions of Article 10. The advising of the person shall be carried out by the individual that will acquaint the above-mentioned persons with the classified information, keeping a written record to that effect.

(3) An authorized person shall be also deemed a person who in proceedings before a state body gets, on the basis of the consent of the head within whose scope the classified information falls, ad hoc gets acquainted with classified information to the extent necessary for the purpose of the proceedings, namely an attorney, public notary, court expert, interpreter, executor or municipality mayor upon signing the non-disclosure declaration and after being advised on their obligations pertaining to the classified information protection and on the potential consequences of their violation. This advising shall be carried out by the person authorized to decide on summoning this person to the proceedings; a written record shall be kept to that effect.

(4) The state body acting in the matter is obliged to notify in writing, without delay, the Authority and the originator of the classified information, of the person pursuant to paragraph 3 and of the scope of their acquaintance with classified information of the Top Secret, Secret or Confidential security classification levels.

---

16) Article 201(2) of Criminal Procedure Code.

17) Act No. 256/1998 Coll. on Witness Protection and on Amendment and Supplementing some Acts, as amended by Act No. 490/2001 Coll.
Article 11 of Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service, as amended.
Article 11 of Act of the National Council of the Slovak Republic No. 198/1994 Coll. on the Military Intelligence, as amended.
Article 41 of Act of the National Council of the Slovak Republic No. 171/1993 Coll. on the Police Force, as amended.
Article 25 of Act No. 240/2001 Coll. on State administration Bodies in Customs, as amended by Act No. 422/2002 Coll.
Article 42 of Act No. 57/1998 Coll. on the Railways Police, as amended.
Article 27 of Act No. 4/2001 Coll. on the Prison and Judiciary Guard Corps, as amended by Act No. 422/2002 Coll.

18a) Article 5(2) of Act No. 69/2018 Coll. on Cybersecurity and on Amendment and Supplementing some Acts.

19) Article 88b of Criminal Procedure Code.

Article 36

(1) Foreign national who is a citizen of a country that has concluded an agreement on the protection of classified information exchanged with the Slovak Republic, may also get acquainted with classified information.

(2) Foreign national pursuant to paragraph 1 may get acquainted with classified information of the security classification levels Confidential through Top Secret only on the basis of a written consent of the head of the state body within whose scope the classified information falls and only after having been issued a certificate by the Authority, unless an international agreement stipulates otherwise.

(3) The Authority shall issue a certificate pursuant to paragraph 2 to a foreign national only after obtaining an opinion pertaining to their security reliability from the competent body of their home country.

(4) The head pursuant to paragraph 2 shall advise the foreign national of the obligations pursuant to this Act and of the potential consequences of their violation, and ensure the person signs a non-disclosure declaration, unless an international agreement stipulates otherwise.

(5) An exception from paragraph 1 may be granted by the Government of the Slovak Republic on the basis of a proposal of the central body of state administration within whose scope the classified information falls, and on the basis of consenting opinions of the Ministry of Foreign Affairs of the Slovak Republic, Ministry of Interior of the Slovak Republic, Slovak Information Service, Military Intelligence and of the Authority.

(6) Paragraphs 1 through 5 apply accordingly to acquaintance with classified information in the case of entrepreneurs from a foreign country.

Article 37

Persons pursuant to Article 36(1) may get acquainted with classified information of the security classification level Restricted only with consent of the state body within whose scope the classified information falls; this body shall determine the scope of acquaintance and ensure the person signs a non-disclosure declaration, unless an international agreement binding upon the Slovak Republic stipulates otherwise.

Article 38

Obligations of Authorized Persons

An authorized person is obliged

a) not to disclose information and objects containing classified information, while they are classified, to unauthorized persons and foreign powers, including after the expiration of the authorization to get acquainted with classified information,

b) to comply with generally binding legal regulation governing the classified information protection,

c) to notify the head without delay of any unauthorized classified information handling and any interest of unauthorized persons in classified information, and to cooperate with the Authority pertaining to clarifying the causes of the unauthorized classified information handling; authorized persons having special status shall notify the Authority of any unauthorized classified information handling and any interest of unauthorized persons in classified information,

d) to notify the head without delay of any change in name and surname, marital status, residence, citizenship and integrity,

e) to notify the head without delay of any fact potentially influencing their authorization to get acquainted with classified information, and of any fact potentially influencing such authorization of another authorized person.

Article 39

Obligations of Unauthorized Persons

(1) An unauthorized person upon obtaining any classified information or classified object is obliged to transfer it without delay to the Authority or to a unit of the Police Force; at the request of the person transferring the classified information or classified object, the recipient shall issue a document on its receipt.

(2) An unauthorized person who becomes acquainted with classified information is obliged to notify this fact without delay to the Authority or to a unit of the Police Force, and to disclose the information with which they have become acquainted.

Article 40

Release from the Non-Disclosure Obligation

(1) A person summoned to testify in proceedings before a state body may be released from the obligation not to disclose classified information by the head of the central body of the state administration within whose scope the classified information falls.

(2) The President of the Slovak Republic, deputy of the National Council of the Slovak Republic, the Prime Minister of the Slovak Republic, the Chairman and Vice-Chairman of the Supreme Audit Authority, judge of the Constitutional Court of the Slovak Republic may be released, for the purpose pursuant to paragraph 1, from the obligation not to disclose classified information with which they have become acquainted with while carrying out their respective functions, by the National Council of the Slovak Republic.

(3) The Attorney General of the Slovak Republic may be released, for the purpose pursuant to paragraph 1, from the obligation not to disclose classified information with which they have become acquainted while carrying out their function, by the President of the Slovak Republic.

(4) A judge may be released, for the purpose pursuant to paragraph 1, from the obligation not to disclose classified information with which they have become acquainted while carrying out their function, by the Judicial Council of the Slovak Republic.

(5) Members of the Government may be released, for the purpose pursuant to paragraph 1, from the obligation not to disclose classified information, by the Prime Minister of the Slovak Republic. Heads of other central bodies of state administration and senior state officials may be released, for the purpose pursuant to paragraph 1, from the obligation not to disclose classified information by the body that elected or appointed them to their office.

(6) A record shall be made in writing on the release of a person from the obligation not to disclose classified information, designating the purpose, scope and period of validity of the release. The head shall send one copy of the record without delay to the Authority; this does not apply to Slovak Information Service, Military Intelligence and to Police Force pertaining to fulfilling criminal intelligence tasks.

(7) Upon a central body of state administration ceasing to exist, a person may be released from the obligation not to disclose classified information by the head of its legal successor; in the absence thereof the person may be released from the obligation not to disclose classified information by the Director of the Authority.

(8) In the case of release from the obligation not to disclose classified information persons pursuant to paragraphs 2 through 5, who are summoned to testify in proceedings before a state body on classified information that fall within the competence of the Slovak Information Service, Military Intelligence and Police Force pertaining to criminal intelligence, the body competent to release these persons of their obligation shall request an opinion from Slovak Information Service, Military Intelligence or Police Force in criminal intelligence.

Article 41

Termination of a Designation

(1) The designation of a person to get acquainted with classified information shall terminate through

a) expiration of the validity of their certificate,

b) termination of the performance of their position,

c) termination of their employment or similar labor relationship, or through the fulfilment of their contractual commitment,

d) revocation of the certificate pursuant to Article 29 within the period for reviewing decision of the Authority pursuant to Article 30,

e) termination of the designation to get acquainted with classified information by the head,

f) completion of compulsory military service or

g) declaration of the person's death.

(2) The head shall prepare a written record on the termination of a designation to get acquainted with classified information, and take measures for their protection.

(3) The head shall notify the Authority of the termination of a person's designation to get acquainted with classified information of the Top Secret, Secret or Confidential security classification levels within 30 days of the termination of this designation.

Article 42

Keeping Records

(1) The Authority shall keep records on authorized persons authorized for Top Secret, Secret and Confidential security classification levels, along with records on persons whose authorization has terminated; this shall not apply to authorized persons who are or have been officers or employees of the Slovak Information Service, Military Intelligence, officers or employees of the Police Force who fulfil criminal intelligence tasks and are kept in their records.

(2) The head shall keep records on authorized persons authorized for the Restricted security classification level, records on persons whose authorization terminated, and a list of authorized persons authorized for the Top Secret, Secret and Confidential security classification levels, and a list of persons whose authorization has terminated.

(3) Records of authorized persons whose authorization to get acquainted with classified information at the security classification levels Top Secret and Secret has terminated, shall be kept for 20 years from the termination of this authorization.

(4) Records of authorized persons whose authorization to get acquainted with classified information at the security classification level Confidential has terminated, shall be kept for three years from the termination of this authorization.

(5) Records of authorized persons whose authorization to get acquainted with classified information at the security classification level Restricted has terminated, shall be kept for one year from the termination of this authorization.

(6) The Authority, Slovak Information Service, Military Intelligence, the Police Force in fulfilling the tasks in criminal intelligence and the heads are obliged under a specific legal regulation[14]) to ensure data protection against unauthorized handling in their records.

(7) Upon expiration of the periods pursuant to paragraphs 3 through 5 the Authority, Slovak Information Service, the Military Intelligence, the Police Force fulfilling tasks in criminal intelligence and the heads shall destroy data kept in archives for the purpose of classified information protection.

(8) The records pursuant to paragraph 1 of the Authority, of the Slovak Information Service, of the Military Intelligence, and of the Police Force in fulfilling tasks in criminal intelligence are records kept pertaining to classified information protection. These records shall not be subject to registration of information systems pertaining to personal data protection.[14])

TITLE III

ENTREPRENEURS

Article 43
Industrial Security

If there is a justified assumption that a state body will require an entrepreneur to create classified information, or if it will be necessary to transfer classified information from a state body to an entrepreneur (hereinafter referred to as the "transfer of classified information"), the entrepreneur is obliged to request the Authority to issue an industrial security clearance certificate.

Article 44
Transfer of Classified Information

(1) Classified information may be transferred by a state body to an entrepreneur who had been issued an industrial security clearance certificate, only on a contractual basis. An employee of an entrepreneur, who is to get acquainted with classified information must be an authorized person for the respective security classification level.

(2) The contract pursuant to paragraph 1 shall contain a specification of the transferred classified information, their security classification level, the period during which the classified information will be transferred, a list of persons, the scope of their authorization to get acquainted with the classified information, the scope of activities involving the classified information, the scope of inspection measures, the obligation to notify of the termination of the entrepreneur or changes affecting the classified information protection, the transfer of the classified information to a different entrepreneur, as well as obligations of the entrepreneur upon the expiration of the industrial security clearance certificate validity.

(3) The state body transferring the classified information is authorized to inspect compliance with their protection also at the entrepreneur to which it transferred the classified information. The results of the inspection shall be incorporated into the annual report prepared pursuant to Article 8(2)o). In the case of identifying shortcomings the transferring body shall be authorized to carry out immediate measures for ensuring the protection of the transferred classified information, including removal of the classified information.

Article 45
Security Clearance of an Entrepreneur

(1) Security clearance of an entrepreneur is carried out by the Authority in order to ascertain, whether the conditions of industrial security pursuant to Article 46 have been met.

(2) The Authority shall carry out security clearance of an entrepreneur on the basis of a request of the entrepreneur's statutory body.

(3) The request for issuance of an industrial security certificate comprises

a) written justification for the request,

b) security classification level and the period of validity for which the certificate is requested,

c) security project of the entrepreneur,

d) entrepreneur's security questionnaire, completed pursuant to Annex No. 3,

e) documents or their certified copies confirming the data in the entrepreneur's security questionnaire,

f) request to carry out a security clearance of the statutory body for the security classification level Confidential, or higher.

(4) The security clearance of an entrepreneur commences on the date of the delivery of the request pursuant to paragraph 3.

(5) (5)If the request has deficiencies due to which it is not possible to carry out the security clearance, the Authority shall interrupt the security clearance and request the entrepreneur to remove them within a designated period; concurrently it shall advise the entrepreneur that in the case of a failure to remove the deficiencies the entrepreneur's security clearance shall be ceased.

(6) The Authority shall interrupt the security clearance of an entrepreneur, if the entrepreneur changed or added during the carrying out of the security clearance person of the statutory body to whom the Authority did not issue a certificate according to Article 26, until completion of security clearance of this person. The Authority shall also interrupt the security clearance if there is an ongoing proceedings in which an issue which might be of significance to completion of security clearance is decided, until the completion of such proceedings.

(7) The Authority shall cease carrying out of the security clearance of an entrepreneur also on the basis of its written request. In this request the entrepreneur is obliged to state the reasons for termination of the security clearance.

(8) The security project of an entrepreneur is a project of a system for classified information protection at the entrepreneur. The security project of an entrepreneur comprises mainly a definition of the security policy and manner of its implementation in personnel security, administrative security, building security and physical security, encryption protection of information, and security of technical devices. It shall also include a list of persons who will get acquainted with classified information.

(9) The Authority, in order to ascertain the industrial security of an entrepreneur, shall request, depending on the nature of the subject-matter, opinions from the Slovak Information Service, Military Intelligence, the Police Force or other body of state administration; these bodies are obliged to comply with the Authority's request. In ascertaining the industrial security of an entrepreneur involved in research, development or production of arms and arms trade, the Authority is obliged to request opinions from the Slovak Information Service, Military Intelligence and the Police Force.

(10) An entrepreneur is obliged, for the purpose of ascertaining its industrial security, to grant officers and employees of the Authority access to buildings and premises, to provide them with requested documents as well as provide true and complete information concerning the facts to be ascertained.

(11) An entrepreneur is obliged to report to the Authority, always by 31 March and 30 September of the calendar year, all changes to data in the entrepreneur's security questionnaire. This obligation shall remain effective during the period of validity of the industrial security clearance certificate.

(12) The Authority is authorized to issue generally binding legal regulation, stipulating the particulars of the entrepreneur's security project.

Article 46

Conditions for Issuing an Industrial Security Clearance Certificate

An industrial security clearance certificate may only be issued to an entrepreneur that is

a) capable of protecting classified information,

b) economically stable,

c) reliable regarding security,

d) being of integrity.

Article 47

An entrepreneur lacking conditions for protecting classified information pursuant to this Act shall not be deemed capable of protecting classified information.

Article 48

An entrepreneur

a) that is in liquidation,

b) against that bankruptcy has been declared,

c) on whose assets settlement has been permitted,

d) that fails to meet financial obligations towards the state or

e) repeatedly fails to meet financial obligations towards other individuals or corporate entities.

shall not be deemed to be economically stable.

Article 49

(1) An entrepreneur at which a security risk has been ascertained, shall not be deemed reliable regarding security.

(2) A security risk shall be deemed to be

a) action against the interests of the Slovak Republic in state defense, state security, international relations, economic interests of the state, functioning of a state body, or against interests that the Slovak Republic has committed to protect,

b) foreign, business or proprietary relation potentially causing detriment to the foreign policy or security interests of the Slovak Republic,

c) the existence of business, proprietary or financial relations with persons pertaining to organized crime,

d) corrupt conduct of the entrepreneur,

e) personnel instability in managing positions or bodies of the entrepreneur or

f) revocation of validity of the certificate of the entrepreneur's head.

Article 49a

For purposes of this Act a person of integrity shall not be deemed an entrepreneur lawfully convicted for a crime unless deemed not to have been convicted. Integrity pursuant to Article 46 d) is proven by an extract from the Criminal Records Register.[10]) For purposes of proving own integrity the entrepreneur shall provide data necessary to request the extract from the Criminal Records Register.[10a]) The Authority shall send the data pursuant to third sentence without delay

electronically via electronic communication to the General Prosecutor's Office of the Slovak Republic to request the extract from the Criminal Records Register.

Article 50

The Industrial Security Clearance Certificate

(1) If the Authority upon carrying out security clearance as certains that the entrepreneur fulfils the conditions pursuant to Article 46, it shall issue an industrial security clearance certificate.

(2) If the Authority upon carrying out security clearance ascertains that the entrepreneur does not fulfil the conditions pursuant to Article 46, it shall issue a decision to that effect.

(3) Validity of the industrial security clearance certificate is five years from the date of issue.

(4) The entrepreneur is authorized to get acquainted with classified information up to the security classification level for which the industrial security clearance certificate has been issued.

(5) If the Authority ascertains that the entrepreneur has ceased to fulfil any of the conditions of industrial security pursuant to Article 46, or has grossly or repeatedly violated own obligations in classified information protection, the Authority shall revoke the validity of the entrepreneur's industrial security clearance certificate.

(6) The provisions of Article 26(3) and (4) and Article 30 apply accordingly to a decision pursuant to paragraphs 2 and 5.

(7) The Authority shall keep a list of entrepreneurs that have been issued industrial security clearance certificates, and a list of entrepreneurs whose industrial security clearance certificates are no longer valid.

Article 51

Period for Issuing an Industrial Security Clearance Certificate

(1) The Authority is obliged to decide on a security clearance of the

a) security classification level Restricted or Confidential within four months from the submission of the request,

b) security classification level Secret or Top Secret within seven months from the submission of the request.

(2) Slovak Information Service, Military Intelligence, Police Force or other state body are obliged to submit their opinion under Article 45(8) to the Authority

a) in the case of a clearance pursuant to paragraph 1 a) within three months from the delivery of the request,

b) in the case of a clearance pursuant to paragraph 1 b) within six months from the delivery of the request.

(3) If it is not possible, given the nature of the matter, to decide in the periods pursuant to paragraph 1, the Authority may extend them by maximum another three months. The Authority is obliged to notify the entrepreneur of the extension to the period, along with a statement of the reasons.

Article 52

Expiration of the Validity of the Industrial Security Clearance Certificate

(1) The validity of the industrial security clearance certificate shall expire through

a) expiration of the period of the industrial security clearance certificate validity,

b) termination of the entrepreneur or

c) notification made pursuant to Article 50(5).

(2) The entrepreneur shall notify the Authority of its termination at latest by the date of its termination.

(3) If the validity of the industrial security clearance certificate has expired pursuant to paragraph 1 b) or c), the entrepreneur shall return it to the Authority within five working days from the date of its expiration or from the date of delivery of the notification pursuant to Article 50(5).

(4) Upon the validity of the industrial security clearance certificate expiring pursuant to paragraph 1, its head shall ensure classified information protection against unauthorized handling.

TITLE IV

PHYSICAL SECURITY AND BUILDING SECURITY

Article 53
Protection of Buildings and Protected Areas

(1) Protection of buildings and protected areas shall be ensured by mechanical prevention devices, technical safeguarding devices, physical protection, regime measures and their mutual combination in accordance with the security standards of physical security and building security.

(2) The manner, conditions and scope of measures proposed for protecting buildings and protected areas shall be determined by the head on the basis of an assessment of the risks of the potential threat.

(3) The head is obliged to secure protected areas in which classified information are discussed.

(4) Protection of buildings and protected areas shall be ensured in accordance with the security documentation of physical security and building security, which shall be approved by the head.

(5) Paragraphs 1 through 4 do not apply to ensuring the placement of special devices, carried out in accordance with specific legal regulations.[20])

(6) If the buildings and protected areas are ensured through technical safeguarding devices enabling audio-, video- or video-audio-recording, their marking pursuant to specific legal regulation on personal data protection shall not be required. This recording shall be destroyed by the person who made it within 60 days after its making unless itis used for purposes of criminal proceedings or offence proceedings.

(7) The Authority is authorized to issue generally binding legal regulation, stipulating the security standards of physical security and building security, and the particulars of protecting buildings and protected areas.

Article 54
Certification of Mechanical Prevention Devices and Technical Safeguarding Devices

(1) Mechanical prevention devices and technical safeguarding devices for classified information protection marked with security classification level Confidential and higher are subject to certification by the Authority.

(2) There are following types of certification:

---

[20]) E. g. Article 88, 88a, 88c and 88d of Criminal Procedure Code, Article 10 of Act No. 46/1993 Coll., Article 39 No. 171/1993 Coll., Article 10 no.198/1994 Coll., Article 37 of Act No. 57/1998 Coll., Article 26 of Act No. 4/2001 Coll., Article 25 of Act No. 240/2001 Coll.

a) certification of a type of mechanical prevention device and certification of a type of technical safeguarding device (hereinafter referred to as "type certification"),

b) certification of an individual mechanical prevention device and certification of an individual technical safeguarding device (hereinafter referred to as "device certification").

(3) The manufacturer,[21])authorized representative of the manufacturer,[21a]) importer[21b]) or distributor[21c]) shall apply to the Authority for issuance of a certificate of a type.

(4) The user shall apply to the Authority for issuance of a device certificate.

(5) A type certificate or device certificate shall be issued for a specific security classification level, and its validity is contingent upon compliance with the conditions and rules of use defined therein.

(6) The validity of a certificate issued for a specific security classification level applies also to lower security classification levels.

(7) The period of validity of a type certificate or device certificate shall be specified by the Authority.

(8) Expenses pertaining to the certification shall be covered by the applicant for certification.

(9) The user of mechanical prevention devices and technical safeguarding devices for classified information protection may continue to use them, in compliance with the conditions stipulated by the Authority, also after the expiry of the validity of the type certificate.

(10) Should the Authority ascertain that a mechanical prevention device or a technical safeguarding device lacks the properties stipulated for the protection of buildings or protected areas, it shall revoke the certificate.

(11) The Authority is authorized to issue generally binding legal regulation, stipulating the particulars of certification mechanical prevention devices and technical safeguarding devices, and of their use.

TITLE V

TECHNICAL DEVICES

First Section

Operational Approval of Technical Devices, Certification and the Security Project

Article 55
Operational Approval

(1) Technical devices may be used only in order to ensure classified information protection.

(2) Technical devices may be used only in compliance with the conditions and rules of use specified in the certificate of the technical device.

(3) Only technical devices given operational approval by the head may be used for work with classified information at a state body or entrepreneur.

---

[21]) Article 2 (3) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (EU OJ L 218, 13.08.2008).

[21a]) Article 2(4) of Regulation (EC) No 765/2008.

[21b]) Article 2(5) of Regulation (EC) No 765/2008.

[21c]) Article 2(6) of Regulation (EC) No 765/2008.

(4) Operational approval may be given only to certified technical devices.

(5) The validity of an operational approval of a technical device for classified information shall be maximum five years for the security classification levels Top Secret and Secret and maximum seven years for the security classification levels Confidential and Restricted.

(6) If serious deficiencies are found in the use of technical devices that was given operational approval, the Authority may through a decision terminate use of the technical devices. Lodging of an appeal against the decision shall have no suspensive effect.

(7) The use of a technical device falling within the competence of the Ministry of Interior of the Slovak Republic, Ministry of Defense of the Slovak Republic or the Slovak Information Service shall be ceased by their heads at the proposal of the Authority.

(8) The use of the technical device may be resumed only with the written consent of the Authority and only after removal of the deficiencies that led to the interruption of use.

(9) The Authority is authorized to issue generally binding legal regulation, establishing the particulars of the operational approval of technical devices, and of their use and detailed requirements placed on technical devices processing classified information.

Article 56

Certification of Technical Devices

(1) Certification of technical devices shall be carried out by the Authority or by a state body authorized by the Authority, or by a corporate entity authorized to certify technical devices; this shall not apply to technical devices used within the competence of the Police Force in connection with fulfilling tasks in operative investigation activity of criminal intelligence, of the Slovak Information Service and the Military Intelligence, where certification shall be carried out by the Ministry of Interior of the Slovak Republic, the Slovak Information Service and the Military Intelligence.

(2) Certification of a technical device shall be contingent upon an assessment of the security project of the technical device.

(3) The certificate of the technical device shall be issued for specific security classification level, and its validity is contingent upon compliance with the conditions and rules of use stipulated therein.

(4) A certificate issued for a certain security classification level is valid also for lower security classification levels.

(5) The validity of the certificate of a technical device for classified information shall be maximum five years for the security classification levels Top Secret and Secret, and maximum seven years for the security classification levels Confidential and Restricted.

(6) Expenses pertaining to certification shall be covered by the applicant for certification.

(7) The Authority is authorized to issue generally binding legal regulation, stipulating the particulars of the procedure in certifying technical devices.

Article 57

System Devices

(1) System protection of classified information of the security classification level Confidential or higher shall, while being processed in technical devices, be ensured by system devices with the recommended security settings.

(2) Assessment of the security settings of system devices shall be carried out by the Authority; this does not apply to system devices used within the competence of Slovak Information Service and Military Intelligence.

(3) System devices subject to security assessment shall include primarily

a) operating systems, their respective versions and modifications,

b) database systems,

c) products for administration and operation of computer networks,

d) products for administration and operation of electronic mail,

e) firewalls and special system security products,

f) other functionally specialized system products designated for creation, processing, transfer or storage of classified information.

(4) Security settings of system devices shall be carried out in accordance with security standards, published by the Authority.

Article 58

Security Project for Technical Devices

(1) The security project for technical devices designates the scope and manner of their use, as well as the means and methods of protecting classified information created, copied or otherwise duplicated, processed, transferred, stored or archived on the technical devices.

(2) The security project for technical devices contains

a) security objective,

b) description of the technical devices,

c) analysis of classified information protection from the aspect of loss, classification violation, accessibility, integrity and authenticity of classified information, classification of the main threats to the classified information, potential countermeasures against respective threats from the aspect of prevention, detection and elimination,

d) use of security standards and designation of other methods and means used for classified information protection,

e) specification of threats taken care of by protective measures and their effectiveness,

f) specification of threats not taken care of by protective measures,

g) guidelines for emergency planning and resumption of operation of the technical device or system.

(3) If possible due to the nature of the technical devices and systems, they shall be protected by using system devices with the recommended security settings, or methods and means of protection in compliance with security standards issued.

(4) The Authority is authorized to issue generally binding legal regulation, stipulating the particulars of drawing up the security project for technical devices and on the issuing and use of security standards.

Second Section

Authorization

Article 59

(1) Consent to the authorization of a state body's or entrepreneur's certification of technical devices and their verifying compliance of mechanical prevention devices and technical safeguarding devices with the security standards of physical security and building security shall be issued by the Authority. Authorization cannot be legally claimed.

(2) An entrepreneur applying for authorization must fulfil the industrial security conditions.

(3) The Authority may issue consent to an authorization the basis of a request of a state body or entrepreneur, provided that the state body or entrepreneur proves that it

a) employs persons professionally qualified to carry out certification,

b) has the premises and technical equipment necessary for carrying out certification,

c) is organizationally capable of ensuring impartiality in carrying out certification activities,

d) has taken out professional liability insurance,

e) is a person authorized or accredited in accordance with specific legal regulation.[22])

(4) In its consent to the authorization of a state body or to the authorization of an entrepreneur the Authority shall state the following

a) name or trade name and registered office,

b) identification number, name,

c) legal form,

d) name, surname and residential address of the person(s) who are the heads of the authorized state body or who are the statutory body of the authorized entrepreneur, or members of such a statutory body, stating the manner and scope of their acting on behalf of the authorized state body or of the authorized entrepreneur,

e) scope and conditions of activities to carried out,

f) period of authorization validity.

(5) The authorized state body or the authorized entrepreneur shall, in the course of certification,

a) carry out technical examinations objectively and at the scientific and technological level representing the state of the art at the time the examinations are carried out,

b) issue concluding protocols on the basis of the technical examinations,

c) notify the Authority without delay of all changes to the conditions designated for authorization.

(6) The authorized state body or authorized entrepreneur is authorized to

a) examine, in carrying out of its activity, the technical, production and other documentation pertaining to the certified device,

b) use on documents issued pursuant to this Act a stamp registered by the Authority,

c) claim reimbursement of its expenses pertaining to the certification from the applicant for certification.

(7) The Authority is authorized to inspect, whether state bodies or entrepreneurs authorized by the Authority comply with the provisions of this Act and with the conditions stated in the consent to the authorization.

(8) If an authorized state body or authorized entrepreneur has ceased to fulfil the conditions stipulated by this Act and the conditions stated in the consent to the authorization, or if it has violated legal regulation pertaining to the scope of its commission or the content of activity, or if an authorized state body or an authorized entrepreneur has applied for such an amendment or termination, the Authority shall amend or revoke its consent to the

---

[22]) E. g. Act No. 264/1999 Coll., Act No. 90/1998 Coll. on Products in Construction, as amended.

authorization. Should an authorized state body or authorized entrepreneur apply for termination of its authorization, it must do so at least six months before the date proposed for termination of the authorization.

(9) An authorized state body or authorized entrepreneur may apply for extension of the validity of the consent to the authorization at least six months before expiration of its validity. The Authority shall extend the validity of the consent to the authorization, if it ascertains that all the conditions pursuant to this Act remain fulfilled by the authorized state body, or by the authorized entrepreneur.

TITLE VI

PROTECTION OF FOREIGN INFORMATION

Article 60
Exchange of Classified Information

(1) Classified information protected by a foreign power and transferred to the Slovak Republic shall be protected pursuant to this Act, if so stipulated by an international agreement binding upon the Slovak Republic or if so required by the accepted principles of multilateral control regimes of which the Slovak Republic is a participant state.

(2) Unless stipulated otherwise herein, classified information of the Slovak Republic may be transferred to a foreign power only in compliance with an international agreement binding upon the Slovak Republic, or if this is required by a resolution of an international organization of which the Slovak Republic is a member state, or if required by the accepted principles of multilateral control regimes of which the Slovak Republic is a participant state, if it is not contrary to other international agreements binding upon the Slovak Republic.

(3) The exchange of classified information between the Slovak Republic and a foreign person shall be carried out in compliance with international agreement binding upon the Slovak Republic.

(4) The Authority shall decide about transfer of classified information between a corporate entity of the Slovak Republic and a foreign entity. The Authority shall, before such transfer, request an opinion from the Ministry of Foreign Affairs of the Slovak Republic, Slovak Information Service, Ministry of Defense, Ministry of the Interior of the Slovak Republic and the central body of state administration within whose scope the classified information falls; these bodies are obliged to comply in writing with the request. The Authority shall also request an opinion from the competent body of the state in which the foreign entity is registered.

(5) The transfer and receiving of classified information shall be carried out through the central register managed by the Authority, unless stipulated otherwise by an international agreement binding upon the Slovak Republic.

(6) In compliance with international agreement binding upon the Slovak Republic, the Authority and the competent authority of the other state are authorized to inspect protection of the mutually transferred classified information.

(7) The Authority shall carry out security clearance of an individual who is to get acquainted with classified information pertaining to fulfilling their tasks pursuant to an international agreement binding upon the Slovak Republic, and shall issue their security clearance certificates; the provisions of Articles 10 through 33 apply to the issuing of such security clearance certificate. If among such individuals there is a person already having undergone security clearance pursuant to Article 18, the Authority shall issue the security clearance certificate on the basis of an assessment of their security file.

(8) Paragraphs 3 through 6 do not apply to the transfer of classified information between the intelligence services of the Slovak Republic and intelligence services of another state, or between the Police Force and police services of another state in the framework of cooperation

carried out pursuant to specific legal regulation;[23]) in such cases consent to the transfer of classified information must be made, and recorded to that effect, by the heads of the intelligence services or by the minister of interior.

(9) Paragraphs 3 through 6 do not apply to the transfer of classified information between armed forces of the Slovak Republic and armed forces of another state, alliance partner or coalition partner or military operation partner within the framework of bilateral cooperation carried out pursuant to specific legal regualtion;[23a])minister of defense decides about transfer of classified information pursuant to previous sentence and keeps a record to that effect.

Article 61

Registers of Classified Information and International Cooperation

(1) In the central register of classified information managed by the Authority shall be recorded all classified information transferred and received in the framework of international cooperation, other than classified information recorded pursuant to Article 60(8).

(2) State bodies and corporate entities transferring and receiving classified information in the framework of international cooperation pursuant to paragraph 1, are obliged, upon obtaining approval, to establish their own registers of classified information, or end register.

Article 62

The Authority shall carry out management and coordination of encryption protection of information in international coordination and exchange of classified information.

TITLE VII

PHOTOGRAPHING, FILMING AND AERIAL PHOTOGRAPHING

Article 63

Prohibition of Photographing and Filming

(1) In the interests of defense and security of the state it is prohibited to photograph, to film or to otherwise make records of buildings, premises or facilities marked by a prohibition on photographing.

(2) Central body of state administration within whose scope the classified information falls, shall decide on the prohibition of photographing, filming or making other records, and exceptions therefrom.

Article 64

Aerial Photographing and Carrying out of Geodesic and Cartographic Works

(1) Aerial photographing of the territory of the Slovak Republic and carrying out of geodesic and cartographic works (hereinafter referred to as “aerial photographing”) shall be carried out by the ministry of defence.[24]) With its consent aerial photographing may also be carried out by an entrepreneur holding a valid industrial security clearance certificate.

(2) The entrepreneur pursuant to paragraph 1shall, within one month, notify the Authority of having acquired aerial photography material, and submit it to the ministry of defense for

---

[23]) E. g. Act of the National Council of the Slovak Republic No. 46/1993 Coll., Act of the National Council of the Slovak Republic No. 171/1993 Coll., Act of the National Council of the Slovak Republic No. 198/1994 Coll., Act No. 256/1998 Coll.

[23a]) Article 11(1) of Act No. 321/2002 Coll on Armed Forces of the Slovak Republic, as amended.

[24]) Article 4 (4) of Act of the National Council of the Slovak Republic No. 215/1995 Coll. on Geodesy and Cartography.

assessing the security classification level of the photographic material. Until such assessment of the aerial photography material it shall be handled as classified information.

PART III

ENCRYPTION PROTECTION OF INFORMATION

Article 65
Central Encryption Authority

(1) Central encryption authority shall coordinate and inspect the activity of central bodies of state administration in encryption protection of information. Pertaining to the intelligence services of the Slovak Republic the inspecting activities of the central encryption authority are limited to the level of departmental encryption authorities and their equivalent encryption authorities.

(2) Central encryption authority shall be authorized to request from central bodies of state administration information necessary to fulfill its tasks.

(3) Unless excluded by this Act or a specific legal regulation, employees of the central encryption authority shall be authorized to enter workplaces of encryption authorities pertaining to inspection of the security of systems and devices used for encryption protection of information.

(4) In case of detecting serious deficiencies in encryption protection of information the central encryption authority may, upon its decision, cease the operation of a system or device used for encryption protection of information. Lodging of an appeal[28]) against the decision has no suspensive effect.

(5) At the proposal of the central encryption authority the head shall cease the operation of a system or device used for the encryption protection of information of the Ministry of Interior of the Slovak Republic, ministry of defense and Slovak Information Service.

(6) Operation of the system or device used for the encryption protection of information may be resumed only upon written consent of the central encryption authority and after removal of the deficiencies that led to the cessation of the operation.

Article 66
Departmental Encryption Authorities

(1) The head of a central body of state administration is authorized to establish, with prior consent of the central encryption authority, a departmental encryption authority as a special workplace for ensuring encryption protection of information within its competence.

(2) Departmental encryption authority shall report directly to the head of the central body of state administration.

(3) The head of the central body of state administration

a) shall be responsible for the encryption protection of information within their competence,

b) shall determine the scope of duties of the departmental encryption authority within their competence and of an encryption authority deemed at the same level,

c) shall approve operation of certified systems and devices for encryption protection of information,

d) shall issue certificates for systems and devices for encryption protection of information for the protection of classified information of the Confidential and Restricted security classification levels,

e) shall cease operation of systems and devices for encryption protection of information in case of detecting deficiencies in the encryption protection of information and shall inform the central encryption authority of the cessation of operation.

Article 67
Certification Authority

(1) To protect classified information, the central encryption authority carry out the function of the certification authority.

(2) In carrying out function pursuant to paragraph 1, the central encryption office shall

a) issue digital certificates,

b) manage digital certificates,

c) provide services pertaining to digital certificates,

d) issue digital certificates to certification authorities operating in closed systems.

Article 68
Professional Qualification

(1) An employee working in encryption protection of information must be a person authorized for acquaintance with classified information pursuant to this Act and must fulfil the conditions of professional qualification.

(2) The employee pursuant to paragraph 1 shall be issued a certificate by the head of the central body of state administration, authorizing them for work in the special workplace of encryption protection of information.

(3) The head of the central body of state administration shall revoke the certificate for work in the special workplace of encryption protection of information of an employee who has ceased to fulfil the conditions pursuant to paragraph 1.

Article 69

The Authority shall be here by authorized to issue generally binding legal regulation, stipulating the particulars of certification and operational approval of systems and devices for encryption protection of information, their use, implementation, transport and registration, use of encryption materials, keeping files on employees in the encryption protection of information and verification of their professional qualification, and details on establishing departmental encryption authorities or encryption authorities deemed at the same level.

PART V

COMPETENCES OF THE AUTHORITY, STATUS, OBLIGATIONS AND POWERS OF OFFICERS OF THE AUTHORITY, COMPETENCES OF THE SLOVAK INFORMATION SERVICE, MILITARY INTELLIGENCE AND THE POLICE FORCE IN CLASSIFIED INFORMATION PROTECTION

Article 70
Competences of the Authority, Status, Obligations and Powers of Officers of the Authority

(1) The Authority shall, in

a) classified information protection

1. elaborate a classified information protection policy and analyses of the state and level of work in this field,

2. carry out inspections on classified information protection,

3. ensure carrying out of security clearance for nominees and security clearance of the President of the Slovak Republic, the Chairman of the National Council of the Slovak Republic and the Prime Minister of the Slovak Republic, if requested so by these persons,

4. issue and revoke certificate of a nominee,

5. carry out training of security employees,

6. issue and revoke industrial security clearance certificate of an entrepreneur,

7. certify technical devices, system devices, mechanical prevention devices and technical safeguarding devices, and issue security standards,

8. authorize state bodies and entrepreneurs to certify technical devices, mechanical prevention devices and technical safeguarding devices,

9. issue security standards,

10. carry out activity of a court expert,

11. maintain records pertaining to classified information protection,

12. issue methodological guidance for activities in classified information protection,

13. ensure tasks pertaining to classified information protection in case state bodies and corporate entities cease to exist without a legal successor,

14. carry out and ensure research and development in information technology security,

b) foreign information protection

1. carry out tasks in classified information protection within the scope stipulated by international agreements,

2. set principles on exchange and protection of classified information in accordance with international agreements under preparation or those in force,

3. inspect compliance with and carrying out of international agreements on exchange of classified information,

4. give its opinion on nominees according to international agreements and issue respective certificates,

5. fulfill tasks pertaining to the central register for exchange of classified information,

6. maintain records pertaining to exchange of classified information,

c) encryption protection of information

1. fulfil the position of central encryption authority of the Slovak Republic,

2. elaborate the policy on the development of encryption protection of information,

3. stipulate principles for encryption protection of information,

4. certify or verify and recognize foreign certificates and approve for operation methods, systems and devices of encryption protection of information for classified information protection at the Top Secret and Secret security classification levels, unless stipulated otherwise herein,

5. recommend or certify or verify and recognize foreign certificates and approve for operation systems and devices of encryption protection of information for classified information protection at the Confidential and Restricted security classification levels,

6. carry out inspections of security of encryption protection of information,

7. designate the conditions for selection, professional preparation of employees and the conditions for the issuance and revocation of work certificates,

8. designate the scope and method of the use of an information system of encryption protection of information,

9. carry out and ensure research and development in cryptology, and research, development and production of devices for encryption protection of information,

10. designate the manner, scope and conditions for administration of systems for encryption protection of information and for the production of encryption materials for systems and devices for encryption protection of information,

11. carry out activity of a court expert,

12. manage records pertaining to encryption protection of information,

13. fulfil the function of the sponsor of the government and foreign connection,

14. fulfil the function of the sponsor of securing devices of encryption protection of information,

15. issue security standards for encryption protection of information and for protection from undesirable electromagnetic radiation of technical devices and devices of encryption protection of information,

e) internal protection, acquire, accumulate, analyze and check information on the security risks pertaining to the scope of competences of the Authority and its officers and employees,

f) public regulated service provided by global satellite navigation system established within the framework of Galileo program, fulfill tasks pursuant to specific legal regualtion.[28c])

(2) The Authority, in fulfilling its tasks under paragraph 1 e), shall be authorized to request from state bodies, corporate entities and individuals assistance, documents and information that may contribute to the prevention and elimination of security risks. No person may be coerced to provide assistance, documents or information.

(3) The Authority may fulfill its tasks pursuant to paragraph 1 also outside the territory of the Slovak Republic, if stemming from international agreements binding upon Slovak Republic or on the basis of the agreement of the parties involved. Decisions on the sending of officers of the Authority for state service abroad are made by the director of the Authority.

(4) In implementing this Act, the Authority shall also cooperate with the national security authorities of other states and security authorities of international organizations.

(5) The Authority shall fulfill its tasks pursuant this Act through its officers who are in a service relationship pursuant to a specific legal regulation.[29])

(6) An officer of the Authority shall prove their affiliation to the Authority by a verbal statement: „National Security Authority“ and by showing their service card, stating the registration

---

[28c]) Article 6(2) e) of Act No. 351/2011 Coll. on Electroincal Communications, as amended by Act No. 247/2015 Coll.

[29]) Act No. 73/1998 Coll. on State Service of Officers of Police Force, Slovak Information Service, Prison and Judiciary Guard Corps of the Slovak Republic and the Railway Police, as amended.

number, name, surname, birth number and photography (hereinafter referred to as „service card“).

(7) An officer of the Authority is obliged, in fulfilling their tasks, to be mindful of the honor, respect and dignity of persons, including themselves, and shall take care to prevent harm or other detriment to persons pertaining to the aforementioned activities.

(8) An officer of the Authority shall be authorized by the director to carry a firearm and use it within the limits of the law for averting an attack directed against them or directly threatening them, or an attack against the life of another person, if it cannot be averted otherwise.

(9) An officer shall, prior to using a firearm, be obliged to call upon the person to cease the unlawful activity and warn the person that a firearm will be used. Prior to using a firearm, the officer shall be obliged to fire a warning shot. The officer may waive the obligation to call upon and to fire a warning shot only when attacked, or where the life or health of another person is threatened in a situation bearing no delay.

(10) In using a firearm an officer shall be obliged to proceed with the necessary caution, in particular to prevent any threat to the life of other persons and to the extent possible spare the life of the person against whom the firearm is used. The officer shall be obliged to report the use of a firearm to their superior.

(11) Tasks of the Authority may also be fulfilled by employees in a labor relationship, the particulars of which are governed by specific legal regulation.[30])

Article 71
Director of the Authority

(1) The head of the Authority is the director of the Authority.

(2) The director of the Authority, upon meeting the requirements pursuant to Article 10, shall be appointed and dismissed by the National Council of the Slovak Republic at the proposal of the Government of the Slovak Republic. The office term of the director of the Authority shall be seven years, commencing from the date of the appointment to the office of the director of the Authority.

(3) The same person may be appointed director of the Authority for maximum two office terms.

(4) The office of the director of the Authority is incompatible with carrying out of an office in another public authority, with employment or a similar labor relationship, with entrepreneurial activities, with membership in a managing or inspecting body of a corporate entity carrying out entrepreneurial activities, or with any other economic or gainful occupation, except for administration of the own property, scientific, pedagogical, journalistic, literary or arts activities.

(5) The carrying out of the office of the director of the Authority shall terminate by expiration of the office term. Prior to expiration of the office term, the office of the director of Authority shall terminate only through

a) resignation from the position,

b) dismissing from the position,

c) death or presumption of death of the director of the Authority.

(6) The director of the Authority may resign from the position through a written notification to the chairman of the National Council of the Slovak Republic. In such a case, the office shall terminate through expiration of the calendar month following the month in which the notification of the director of the Authority on the resignation from the position was received by the chairman of the National Council of the Slovak Republic, if not agreed otherwise

[30]) Labor Code, as amended.

pertaining to the date of termination of the office of the director of the Authority between the chairman of the National Council of the Slovak Republic and the director of the Authority.

(7) National Council of the Slovak Republic may dismiss the director of the Authority from the position on the basis of a proposal of 30 deputies, or at the proposal of the Government, or if the director of the Authority

a) has failed to remove reasons for incompatibility stipulated in paragraph 4 within three months from appointment to the office,

b) has started to carry out an activity or a position incompatible with the office,

c) has been convicted for a criminal offence by lawful court decision,

d) has been lawfully incapacitated, or their legal capacity has been restricted,

e) has lost citizenship,

f) has become a member of a political party or a political movement,

g) has been unable for more than one year to carry out the office for health reasons pursuant to a medical ruling, decision of a body of the national health authority or a social care body,

h) has no permanent residence in the territory of the Slovak Republic,

i) lost the authorization to get acquainted with classified information pursuant to Articles 28 and 29.

(8) The director of the Authority shall be dismissed from the office from the day following the day when the decision of the chairman of the National Council of the Slovak Republic about the dismissal from the office has been delivered.

(9) The director of the Authority shall have six weeks of leave in a calendar year. For the time of leave the director of the Authority shall be paid regular salary.

(10) The director of the Authority shall prove the own identity during the official activities by a service card issued by the Authority.

(11) All documents pertaining to the function of the director of the Authority shall be filed to the personnel file maintained by the Authority. The personnel file is kept for the period of 50 years after leaving this position.

(12) The provisions of part VI and VIII and Articles 110 through 112, 122 through 128 and 141 of the specific legal regulation[29]) apply accordingly, for the director of the Authority while carrying out this office.

Article 71a

Salary Particulars, Material Benefits and Lump-Sum Compensations of the Director of the Authority

(1) The Director of the Authority shall be assigned monthly a salary of the monthly salary of a deputy of the National Council of the Slovak Republic[30a])starting on the first day of the month in which he was elected. Director of the Authority shall be assigned a compensation of three-fold of the monthly salary of the last monthly salary. The salary shall be rounded up to the whole euro.

(2) The Director of the Authority while at the position has got a right to free

[30a]) Article 2 of act of the National Council of the Slovak Republic No. 120/1993 Coll. on Salary Particulars of some Constitutional Officials in the Slovak Republic, as amended.

a) use of an official vehicle assigned with or without a driver to carry out the office, or in connection therewith,

b) the provision and use of mobile phone device to ensure accessibility when being in and out of the office.

(3) The Director of the Authority shall be assigned a monthly lump-sum compensation of 54% of the monthly salary to cover the necessary expenses for services and other expenses pertaining to his position. The lump-sum compensation is designated by a fixed amount rounded up to the whole euro.

(4) The Government of the Slovak Republic Government may assign the Director of the Authority a reward for good performance of tasks or fulfillment of extraordinary tasks, important tasks or pre-defined tasks.

(5) For the purposes of health insurance, hospital insurance and pension insurance, the Director of the Authority shall deemed an employee in labor relationship.

Article 72

Supervision of the Authority by the National Council of the Slovak Republic

(1) Supervision over the activities of the Authority shall be carried out by the National Council of the Slovak Republic, which shall, for this purpose, establish a special supervision body (hereinafter referred to as the "Supervision Body") consisting of deputies.

(2) Members of the Supervision Body are authorized, accompanied by an officer of the Authority, to enter protected areas of the Authority and get acquainted with classified information pertaining to the activities of the Authority, unless an international agreement binding upon the Slovak Republic stipulates otherwise.

(3) Should the Supervision Body, in exercising its powers, find any violation of this Act, it shall be obliged to notify the National Council of the Slovak Republic and Attorney General of the Slovak Republic; according to the nature of the matter, it shall inform also the Government of the Slovak Republic.

(4) Unless stipulated otherwise herein, a specific legal regulation[31]) shall apply to the proceedings of the Supervision Body and to its rights and the obligations of its members accordingly.

Article 73

(1) National Council of the Slovak Republic shall elect at the beginning of each electoral term members of the Supervision Body and designate the number of its members, composition and manner of this body's work.

(2) Should a deputy, a member of the Supervision Body, leave the club of deputies, they shall lose membership in this body. As a replacement, the club of deputies shall propose a new member.

(3) Meetings of the Supervision Body are not public. The Supervision Body shall meet at least quarterly. During its sessions it shall proceed according to its rules of procedure. Every member of the Supervision Body may request its convocation.

(4) The Supervision Body shall perform its activity even after the end of the election term of the National Council of the Slovak Republic until the National Council of the Slovak Republic elects a new Supervision Body for the new election term.

---

[31]) Act of the National Council of the Slovak Republic No. 350/1996 Coll. on Rules of Pprocedure of the National Council of the Slovak Republic, as amended.

Article 74

(1) Fact that the members of the Supervision Body got acquainted with in exercising their powers, may only be transferred in the extent necessary for achieving the purpose of supervision pursuant to this Act.

(2) Members of the Supervision Body shall be obliged not to disclose the facts of which they have learnt in carrying out their position. The obligation not to disclose facts shall also continue after the member of the Supervision Body do not exercise the position anymore, and only the National Council of the Slovak Republic may release them from this obligation.

Article 75

Slovak Information Service and Military Intelligence

(1) Slovak Information Service and Military Intelligence shall

a) carry out security clearances of nominees within their respective competences pursuant to Article 18,

b) at the request of the Authority, provide the Authority with information on the security reliability of nominees from their records,

c) at the request of the Authority carry out security checks, within the scope of their respective competences, on the reliability of nominees at the place of residence of the nominee, and provide information from these checks to the Authority,

d) at the request of the Authority, within the extent of their respective competences, carry out security checks of the environs where the nominee lives, the occurrence of potential security risks and provide the information from these checks to the Authority,

e) at the request of the Authority provide information on an individual pursuant to Article 69a (2) for ascertaining the judicial eligibility requirements and carry out to that effect checks in the place of permanent residence pursuant to Article 69a(2) and security checks of the environs where this individual lives and associates,

f) at the request of the Authority provide information required to determine the industrial security of corporate entities,

g) approve into the operation and certify technical devices used exclusively within their respective competences,

h) maintain records pertaining to classified information protection,

i) maintain registers of classified information, transferred and received within the framework of international cooperation,

j) carry out training of their security employees.

(2) Slovak Information Service and Military Intelligence shall be authorized, in carrying out their tasks pursuant to paragraph 1, to

a) use data from their records and from records and materials stemming from activities of security authorities and military authorities or request such data,

b) acquire necessary information from state bodies, municipalities and corporate entities,

c) maintain in their records data acquired while carrying out their tasks pursuant to this Act.

(3) Slovak Information Service and Military Intelligence shall be authorized to apply information-operational means pursuant to a specific legal regulation[32]) in carrying out security

[32]) Act No. 166/2003 Coll. on the Privacy Protection from Unauthorized Use of Information-Technological Devices and on the Amendment of some Acts (Act on the Protection from Bugging)

clearances of the 3rd and 4th degrees and in acquiring information in order to ascertain industrial security.

(4) Slovak Information Service shall certify and approve into operation methods, systems and devices for encryption protection of classified information at the Top Secret and Secret security classification levels, intended for the provision of classified information by the Slovak Information Service to intelligence services of other states within cooperation carried out pursuant to a specific legal regulation; such certification and approval into operation shall be carried out in accordance with the generally binding regulation issued by the Authority pursuant to Article 69.

Article 76

Police Force

(1) Police Force shall

a) at the request of the Authority, provide the Authority with information from its records on the security reliability of nominees,

b) at the request of the Authority, carry out security checks on the reliability of nominees at the place of residence of the nominee, and provide information from these checks to the Authority,

c) at the request of the Authority, carry out security checks of the environs where the nominees live, the occurrence of potential security risks and provide the information from these checks to the Authority,

d) at the request of the Authority, provide information to ascertain the industrial security of corporate entities.

(2) In carrying out its tasks pursuant to paragraph 1, the Police Force shall be authorized to

a) use data from its records,

b) acquire the necessary information from state bodies, municipalities and corporate entities.

(3) Police Force in fulfilling criminal intelligence[33]) tasks shall be authorized, in carrying out security clearances pursuant to Article 18(4), to use means of operative-investigative activities and apply information-technical devices, and to keep security files on their officers and employees.

PART VI

INSPECTIONS AND LIABILITY FOR VIOLATION OF OBLIGATIONS

Article 77

Inspections

(1) Unless stipulated otherwise herein, the Authority shall, in inspecting the classified information protection in state bodies, municipalities, higher territorial units and other corporate entities, proceed as in carrying out an inspection in the state administration pursuant to a specific legalregulation.[34])

(2) In carrying out inspection activities, officers and employees of the Authority shall be authorized to

---

[33]) Act of the National Council of the Slovak Republic No. 171/1993 Coll., as amended.

[34]) Act of the National Council of the Slovak Republic No. 10/1996 Coll. on Inspections in State Administration, as amended.

a) get acquainted with classified information at all security classification levels to the extent necessary for the inspection,

b) enter information systems up to the system administrator level to the extent necessary for the inspection,

c) enter all buildings and protected areas holding classified information,

d) propose revocation of the validity of a certificate of a person authorized to get acquainted with classified information and of an entrepreneur's industrial security clearance certificate,

e) carry out measures bearing no delay for ensuring classified information protection, including the removal of classified information,

f) request that shortcomings ascertained be removed by a designated deadline and a written report on their removal be sent to the Authority.

(3) The provisions of paragraph 2, except for those of subparagraphs d) through f) also apply to the carrying out of activities of a court expert and the preparation of methodology.

(4) Everyone shall be, in cases pursuant to paragraph 2e), obliged to comply with the summons of an officer or employee of the Authority to surrender classified information.

Article 78
Offences

(1) An authorized person violating an obligation pursuant to Article 38 commits an offence in the field of classified information protection.

(2) An offence in classified information protection is also committed by a person who as an unauthorized person

a) fails not to disclose classified information with which they got acquainted,

b) fails to comply with the obligation to give notice of information that has become known to them, or the obligation to surrender an object found, containing classified information,

c) breaches the prohibition of photographing, filming or making other records of buildings, premises or facilities,

d) uses technical device contrary to the provisions of this Act,

e) carries out unauthorized aerial photographing of the territory of the Slovak Republic.

(3) A fine may be imposed for an offence

a) pursuant to paragraph 1, of up to SKK 50 000 or the prohibition of activities,

b) pursuant to paragraph 2a) and b), of up to SKK 15 000,

c) pursuant to paragraph 2c), d) and e), of up to SKK 50 000.

(4) Offences in classified information protection shall be dealt with by the Authority.

(5) Offences and the proceedings pertaining to them shall be regulated by a specific legal regulation.[35])

[35]) Act of the National Council of the Slovak Republic No. 372/1990 Coll. on Offences, as amended.

Article 79

Administrative Infractions

(1) A corporate entity violates obligations in of classified information protection, if it

a) provides classified information to a foreign power contrary to an international agreement binding upon the Slovak Republic,

b) fails to maintain proper records on persons authorized to get acquainted with classified information and on persons whose authorizations to do so have terminated,

c) fails to notify the Authority, within the period stipulated pursuant to this Act, of the termination of the authorizations of persons to get acquainted with classified information of the Top Secret, Secret or Confidential security classification levels,

d) fails to inform the Authority on the designation of authorized persons for the Top Secret, Secret and Confidential security classification levels,

e) fails to inform the Authority of the commencing of the carrying out of tasks in research, development, design and production that constitute classified information of the Top Secret, Secret or Confidential security classification levels,

f) fails to notify the Authority of the concluding of an international agreement or business contract the subject matter of which represents classified information, with a foreign entity or with the co-participation of a foreign entity,

g) fails to ensure conditions required for classified information protection,

h) fails to ensure proper record-keeping, transport, storage, disposal and archiving of information and objects containing classified information,

i) performs unauthorized aerial photographing of the territory of the Slovak Republic, or violates state defense interests in performing geodesic and cartographic works,

j) violates any obligation imposed pursuant to this Act in encryption protection of information,

k) uses a technical device contrary to the provisions of this Act.

(2) For the violation of obligations stipulated in paragraph 1a) through d) a fine may be imposed of up to SKK 500 000, and for the violation of those set out in paragraph 1e) through k) a fine of up to SKK 1 000 000 may be imposed.

(3) A fine of up to double the amounts set out in paragraph 2 may be imposed for the simultaneous violation of several obligations in classified information protection.

(4) For the repeated violation of obligations in classified information protection stipulated pursuant to paragraph 1 a further fine may be imposed of up to double the amounts stipulated pursuant to paragraphs 2 and 3 within the period of two years from the date of the law full validity of the decision on the imposition of the previous fine.

Article 80

Imposition of Fines

(1) The Authority shall in administrative proceedings impose fines for the violation of obligations pursuant to Article 79. In determining the fine, the Authority shall take into account the gravity, manner, duration and consequences of the unlawful action.

(2) The fine may be imposed within one year from the date when the violation of obligations in classified information protection became known to the Authority, but not later than three years from the date of the violation.

(3) The fine shall be payable within 30 days from the date of the decision on its imposition taking effect.

(4) The imposition of a fine pursuant to Articles 78 and 79 shall not prejudice the provisions of specific legal regulation on the compensation of damages[36]) nor shall obligations stipulated pursuant to this Act cease to apply.

(5) Fines shall be revenues of the state budget.

PART VII

COMMON, TRANSITIONAL AND CONCLUDING PROVISIONS

Common Provisions

Article 81

(1) Generally binding legal regulation on administrative proceedings[37]) shall not apply to decision making pursuant to this Act, except for Article 55(6), Article 65(4), Articles 79 and 80.

(2) The term "state secret" or "service secret" used in laws and other generally binding legal regulation shall mean "classified information".

(3) For the purposes of this Act the Supreme Audit Office of the Slovak Republic, the Office of the Attorney General of the Slovak Republic, the Slovak Information Service, the Military Intelligence, the National Bank of Slovakia, the Office of the President of the Slovak Republic, the Office of the National Council of the Slovak Republic, the Office of the Constitutional Court of the Slovak Republic and the Office of the Supreme Court of the Slovak Republic have the status of central bodies of state administration.

Article 82

The term "Authority", pursuant to Article 8(2)f),h),j) through m), Article 9(1), Article 10(1)h), Articles 24 through 29, Article 31(3), Article 33, Article 42(1) and Article 78(4) shall mean the Slovak Information Service, Military Intelligence and the Police Force pertaining to persons subject to security clearance pursuant to Article 18(1), (2) and (4); and the term "Authority", pursuant to Article 8(2)f),h),j) through m), Article 9(1), Article 10(1)(h), Articles 24 through 25, Article 33, Article 42(1) and Article 78(4), shall mean the Military Intelligence pertaining to persons subject to security clearance pursuant to Article 18(3).

Article 83

The provisions of Article 8(2)f),h),j) through m), Article 16(1)b) through f), Article 31(3), Article 32(2), Article 41(3), Article 70(1)a) items 4 and 11, Article 77(2)b) and e) and Article 79(1)c), d), e) and k) shall not apply to the Slovak Information Service, Military Intelligence and the Police Force pertaining to fulfilling the tasks in criminal intelligence.

Article 84
Transitional Provisions

(1) Unless stipulated otherwise, classified information pursuant to legal regulation in force until now shall remain classified information pursuant to this Act.

(2) Proceedings on the imposition of fines for violation of obligations in classified information protection commenced prior to the effect of this Act shall be completed by the Authority in accordance with legal regulation in force hitherto.

---

[36]) E. g. Civil Code as amended, Labour Code as amended.
[37]) Act No. 71/1967 Coll., as amended.

(3) A person designated as of 1 November 2001 to get acquainted with service secrets shall be deemed a person authorized for the security classification level Confidential or Restricted pursuant to this Act until 31 October 2004, unless other circumstances arise causing the termination of the authorization.

(4) The certificate of an employee in encryption protection of information, issued prior to 1 November 2001 shall be deemed a certificate of the employee in encryption protection of information issued pursuant to this Act, and its validity shall expire at the latest on 31 December 2004.

(5) A public prosecutor, heads of other central bodies of the state administration, senior state official and the Chairman of the Office for Protection of Personal Data shall be persons authorized to get acquainted with classified information pursuant to this Act until the expiration of their terms of office, but at the latest until 31 December 2006, unless a specific Act stipulates otherwise; this provision shall not prejudice the issuance of certificates under Article 60(7).

(6) Uncertified mechanical prevention devices and uncertified technical safeguarding devices put into operation pursuant to hitherto legal regulation may be used for protecting buildings and protected areas until 31 December 2005.

(7) An information encryption protection device used for protection of information forming the subject matter of a state secret or of a service secret pursuant to legal regulation in force hitherto shall be deemed a certified device for encryption protection of information pursuant to this Act until 31 December 2004, provided that the approval decision was issued by 31 October 2001.

(8) Departmental encryption authorities established in accordance with legal regulation valid hitherto shall be deemed departmental encryption authorities established pursuant to this Act.

(9) A statement of the Authority issued according to legal regulation in force hitherto shall be deemed a certificate pursuant to this Act for the period of validity stipulated therein. A person so authorized to get acquainted with classified information may apply to the Authority for issuance of the certificate if they prove important interest for its issuance; this does not apply to a person subject to security clearance of all security classification levels by the Slovak Information Service, Military Intelligence or the Police Force pursuant to legal regulation in force hitherto.

(10) Security clearance of a nominee commenced according to hitherto in force legal regulation shall be completed pursuant to this Act.

(11) Court proceedings commenced before this Act enters into force shall be completed pursuant to legal regulation hitherto in force.

(12) An industrial security clearance certificate issued pursuant to legal regulation hitherto in force shall be deemed an industrial security clearance certificate issued pursuant to this Act.

(13) Security clearance of an entrepreneur commenced according to hitherto legal regulation shall be completed according to hitherto legal regulation.

(14) A briefing certificate of the Authority on the classified information protection issued pursuant to hitherto legal regulation shall be deemed a certificate pursuant to Article 9 of this Act until 30 April 2005.

(15) A certificate issued by the Authority according to hitherto legal regulation shall, for the period of validity stated therein, be deemed a certificate issued pursuant to this Act.

(16) An authorization issued by the Authority according to hitherto legal regulation shall, for the period of validity stated therein, be deemed an authorization issued pursuant to this Act.

(17) The appointment of the Director of the Authority who has been in this position pursuant to hitherto legal regulation, shall be deemed an appointment pursuant to this Act.

Article 84a

A security clearance commenced pursuant to the provisions of this Act, effective before 1 February 2008, will be completed in accordance with the provisions of this Act, effective since 1 February 2008.

Article 84c

Transitional Provisions as of 1 January 2015

The Director of the Authority shall be assigned in the year 2015 the regular salary at the amount of the salary of the deputy of National Council of the Slovak Republic stipulated for year 2015.[38])

Article 84d

Transitional Provisions as of 1 January 2016

The Director of the Authority shall be assigned in the year 2016 the regular salary at the amount of the salary of the deputy of National Council of the Slovak Republic stipulated for year 2016.[39])

Article 84e

Transitional Provisions as of 1 July 2016

A security clearance of an entrepreneur commenced pursuant to the provisions of this Act, effective before 1 July 2016, will be completed in accordance with the provisions of this Act, effective since1 July 2016.

Article 84g

Transitional Provisions as of 1 January 2018

The Director of the Authority shall be assigned in the year 2018 the regular salary at the amount of the salary of the deputy of National Council of the Slovak Republic stipulated for year 2018.[41])

Article 85

Repealing Provisions

The following shall be repealed:

1. Article I of Act No. 241/2001 Coll. on Classified Information Protection and Amendment and Supplementing some Acts, as amended by Acts No. 418/2002 Coll., No. 432/2003 Coll. and No. 458/2003 Coll.,
2. National Security Authority Decree No. 432/2001 Coll. laying down the List of Classified Information,
3. National Security Authority Decree No. 455/2001 Coll. on Administrative Security,
4. National Security Authority Decree No. 2/2002 Coll. on Personnel Security,
5. National Security Authority Decree No. 28/2002 Coll. on Industrial Security,
6. National Security Authority Decree No. 88/2002 Coll. on Physical Security and Building Security,

---

[38]) Article 29l of Act of the National Council of the Slovak Republic No. 120/1993 Coll. as amended by Act No. 362/2014 Coll.

[39]) Article 29 n of Act of the National Council of the Slovak Republic No. 120/1993 Coll. as amended by Act No. 338/2015 Coll.

[41]) Article 29o of Act of the National Council of the Slovak Republic No. 120/1993 Coll. as amended by Act No. 334/2017 Coll.

7. National Security Authority Decree No. 89/2002 Coll. adjusting details on the Certification and Use of Mechanical Prevention Devices or Technical Safeguarding Devices,

8. National Security Authority Decree No. 90/2002 Coll. on the Security of Technical Devices,

9. National Security Authority Decree No. 91/2002 Coll. laying down Details on the Encryption Protection of Information.

Article II

Slovak National Council Act No. 71/1992 Coll. on court fees and the fee for a judicial extract, as amended by National Council of the Slovak Republic Act No. 89/1993 Coll., National Council of the Slovak Republic Act No. 150/1993 Coll., National Council of the Slovak Republic Act No. 85/1994 Coll., National Council of the Slovak Republic Act No. 232/1995 Coll., Act No. 12/1998 Coll., Act No. 457/2000 Coll., Act No. 162/2001 Coll., Act No. 418/2002 Coll., and Act No. 531/2003 Coll. shall be supplemented as follows:

In Article 4(2)(j), a comma and the words “members of the National Security Authority and members of the Slovak Information Service” shall be inserted after the words “the Slovak Republic”.

Article X

Act No. 253/1998 Coll. on reporting the residential addresses of citizens of the Slovak Republic and on the Residency Register of the Slovak Republic, as amended by Act No. 369/1999 Coll., Act No. 441/2001 Coll., and Act No. 660/2002 Coll. shall be supplemented as follows:

Article 25 shall be supplemented with paragraph 3, worded as follows:

“(3) The National Security Authority, the Slovak Information Service, the Military Intelligence Service and the Police Force are empowered to extract from the records of residential addresses of citizens (Article 11) and from the Register (Article 13) data in connection with the performance of security clearances pursuant to specific regulations.[11a)] Details on the procedure in extracting the aforesaid data shall be agreed upon between the Ministry and the National Security Authority in a separate agreement.”.

The footnote 11a) shall be worded as follows:

“[11a)] Act No. .../2004 Coll. on the protection of classified information and on the amendment and SupplementingActs”.

Article XII

Act No. 314/2001 Coll. on fire prevention, as amended by Act No. 438/2002 Coll. shall be supplemented as follows:

In Articles 43(1), 45(3), 48(1)(a), a comma and the words “the National

1. Security Authority,” shall be inserted after the words “of the Railway Police,”..

2. In Article 66(1)(a), the words “of the National Security Authority,” shall be inserted after the words “of the Railways Police,”.

3. The footnote 14 shall be supplemented with the following words at the end of the quotation: “Article 138 of Act No. 73/1998 Coll. on state service of the members of the Police Force, the Slovak Information Service, the Prison and Judicial Guard Corps of the Slovak Republic and the Railways Police, as amended.”.

Article XIII

Act No. 315/2001 Coll. on the Fire Brigade and Rescue Corps, as amended by Act No. 438/2002 Coll., Act No. 666/2002 Coll., Act No. 424/2003 Coll., Act No. 451/2003 Coll., and Act No. 462/2003 Coll. shall be supplemented as follows:

In Article 8(3) a comma and with the words “the National Security Authority” shall be inserted after the words “the Railways Police”.

Article XIV

Act No. 540/2001 Coll. on state statistics shall be supplemented as follows:

In Article 31(1)(d), the words “other central bodies of the state administration” shall be inserted after the word “ministries”.

Article XV

Act No. 564/2001 Coll. on the public protector of rights, as amended by Act No. 411/2002 Coll. and Act No. 551/2003 Coll., shall be amended as follows:

1. In Article 12(1), the words “and in the matters of classified information,(5)” after the words “of a personality” shall be deleted. At the same time the footnote (5) shall be deleted.

2. In Article 12 the paragraph 3 shall be deleted. At the same time the footnote (7) shall be deleted.

Article XVII

Act No. 483/2001 Coll. on Banks and on the Amendment of some Acts, as amended by Act No. 430/2002 Coll., Act No. 510/2002 Coll., Act No. 165/2003 Coll., Act No. 483/2001 Coll., and Act No. 603/2003 Coll., shall be supplemented as follows:

In Article 91(4), the following point (l) shall be inserted:

“(l) of the National Security Authority, the Slovak Information Service, the Military Intelligence Service and the Police Force for the purposes of carrying out the security clearances under a specific regulation.86a)”.

The footnote 86a) shall have the following text:

“86a) Article 19 of Act No. .../2004 Coll. on Classified Information Protection and on Amendment and Supplementing of some Acts.”.

Article XIX

Act No. 350/1996 Coll. on the rules of procedure of the National Council of the Slovak Republic as amended by Act No. 77/1998 Coll., Act No. 86/2000 Coll., Act No. 138/2002 Coll., Act No. 100/2003 Coll. and Act No. 551/2003 Coll., shall be supplemented as follows:

1. In Article 60(1) the words “of the National Security Authority and” shall be inserted after the word “activities”.

2. At the end, in the footnote (30), the words: “Article 72 of Act No. .../2004 Coll. on the protection of classified information and on the amendment of some Acts” shall be added.

3. At the end, in the footnote (50), the words: “Article 72 of Act No. .../2004 Coll. on the protection of classified information and on the amendment of some Acts” shall be added.

Article XX

Act No. 575/2001 Coll. on the organization of activities of the Government and organizations of central state administration, as amended by Act No. 575/2001 Coll., Act No. 143/2002 Coll., Act No. 411/2002 Coll., Act No. 465/2002 Coll., Act No. 139/2003 Coll., Act No. 453/2003 Coll. and Act No. 523/2003 Coll., shall be amended as follows:

Article 22(8) shall have the following wording:

"(8) At the head of the National Security Authority shall be the Director, who shall be appointed and recalled by the National Council of the Slovak Republic according to a specific regulation,1c)".

Footnote (1c) shall have the following text:

"(1c) Article 71 of Act No. .../2004 Coll. on the protection of classified information and on the Amendment of some Acts.".

Article XXI

Force of legislation

This Act enters into force on 1 January 2004.

President of the Slovak Republic

Chairman of the National Council of the Slovak Republic

Prime Minister of the Slovak Republic

Annex No. 1 to Act No. 215/2004 Coll.

State Security Structures Pursuant to Article 14(1)

Pursuant to this Act an officer who performed activities in the following units shall be deemed a person assigned to a position in the past State Security structures:

1. Chief Directorate of State Security (1966-1971),

2. Federal Directorate of Intelligence Services (1969-1971),

3. Secretariat of the Deputy Minister of Interior of the Czechoslovak Socialist Republic,

4. Security Division of the Ministry of the Interior (MoI) of the Slovak Socialist Republic (SSR) (1969-1971),

5. Security Organisation Section of MoI of the Czech Socialist Republic (ČSR) (19691971),

6. Chief Directorate of State Security (ŠtB) of the MoI SSR (1969-1974),

7. MoI Security Presidium (1948-1950),

8. Division BA of Group I – Security of the MoI (1948-1950),

9. ŠtB Headquarters (1950-1952),

10. Chief Directorate of the Military Counter-Intelligence Service (1952-1953),

11. State Security Investigations Directorate (1953),

12. ŠtB Regional Headquarters (1950-1952) and their subordinated units,

13. MoI Directorate II (1953-1963),

14. MoI Directorate II (later of Federal MoI, 1964-1974),

15. MoI Directorate III (1953-1963),

16. MoI Directorate IV (1953-1963),

17. MoI Directorate V (1952-1962),

18. MoI Directorate VI (1953-1963),

19. Federal MoI Directorate XI (later ZNB),

20. 1st, 2nd, 3rd, 4th, 5th independent sector of the Ministry of National Security (1950-1951),

21. Divisions O, Z, C, E, T, V, LM of the Ministry of National Security (1951-1952),

22. Operative divisions and departments of the Presidential Protection Directorate (1952-

23. 1953), Constitutional Officials Protection Directorate (1952-1953), MoI Directorate VIII,

24. Operative division of MoI Directorate VII (1953-1963), MoI Directorate IV (later FMoI),

25. Division of MoI Directorate VII, authorized to carry out arrests and domestic searches (1953 - 1956),

26. Operative divisions of MoI Directorate XI (1953-1963) and MoI Directorate VI (later FMoI),

27. National Security Corps (ZNB) Directorate I,

28. ZNB Directorate II,

29. ZNB Directorate X (1974-1988),

30. ZNB Directorate XI (1974-1988),

31. ZNB Directorate III (1964-1990),

32. ZNB Directorate IV (1964-1990),

33. ZNB Directorate VI (1964-1990),

34. Main Directorate of Military Counter-Intelligence Service (1.9.1970-31.8.1983),

35. ZNB Directorate XII (1974-1990),

36. ZNB Directorate XIII,

37. ZNB Directorate XIV,

38. Federal Directorate of the ŠtB Investigation,

39. ŠtB Directorates of ZNB regional directorates, except for the members of the Czechoslovak aircraft escort department of the airport control division,

40. ŠtB departments of the ZNB district directorates, except for the members of the regime protection of nuclear power stations.

Annex No. 2 to Act No. 215/2004 Coll.

Personal Questionnaire of a Person

Personal questionnaire of a person consists mainly of:

1. Personal data of the nominee.

2. Data on residence.

3. Contact data.

4. Identity documents.

5. Marital status.

6. Education and an overview of schools attended.

7. Present employment, previous employment or registered employment seeking.

8. Entrepreneurial activity or activity carried out pursuant to specific legal regulation.

9. Personal data of spouse, children, spouse's children and other persons living in the same household.

10. Criminal proceedings, offence proceedings, disciplinary proceedings and any other proceedings against nominee.

11. Undergone psycho-physiological examination of truthfulness.

12. Cooperation with the State Security and Intelligence Administration of the General Headquarters of the Czechoslovak People Army until 31 December 1989.

13. Opinion pertaining to the requirements for inception of an auhtorization to get acquainted with classified information pursuant to Articles 10 through 14.

Annex No. 3 to Act No. 215/2004 Coll.

Security Questionnaire of a Person

A. General Part

Security questionnaire of a person consists mainly of:

1. Data on military service.

2. Personal data of parents and siblings.

3. Facts pertaining to possible present of previous addiction on alcoholic beverages and present or previous usage of narcotic drugs, psychotropic substances and other material substances.

4. Facts on present or previous gaming addiction.

5. Psychiatric examinations and therapies.

6. Property.

7. Registered enforcement decisions.

8. Lawful decisions of public authorities and other corporate entities, imposing a monetary obligation.

9. Acquainting with classified information.

10. Cooperation or other contacts to previous or present intelligence service of foreign power.

11. Cooperation or other contacts to persons or entities, whose activity is aimed against democratic social order or against interests which the Slovak Republic is bound to protect based on international agreements.

12. Statutory declaration pertaining to truthfulness of the stated data.

13. Consent with providing information from the health file.

B. Supplementary part to be completed only for Top Secret and Secret security classification levels

1. Personal data of other family members - parents of the spouse, of the common-law spouse, siblings of the spouse.

2. Membership of, and relationship to civic associations, political movements and parties, churches, religious societies, domestic and foreign entities.

3. Identification and contact data of two individuals familiar with the nominee, able to provide information on the data in the personal and security questionnaire of a person (family members or persons with confidential relations, e.g. managing common property, are not eligible).

4. Stays abroad longer than 30 days after reaching 18 years of age.

Annex No. 4 to Act No. 215/2004 Coll.

Security Questionnaire of an Entrepreneur

Security questionnaire of an entrepreneur consists mainly of:

1. Identification data of the entrepreneur.

2. Economic data of the entrepreneur.

3. Property data of the entrepreneur.

4. Business relations of the entrepreneur.

5. Petitions for bankruptcy, settlement, entry into liquidation or destructuralization.

6. Identification data of members of statutory body.

7. Corporate entities, where the members of the statutory body were or are associates, managing directors, members of the supervisory board or members of the board.

8. Identification data of associates, limited partner, general partners, members of cooperative societies, members of supervisory board, agent, member of the management board in the last five years, of the founding members and identification data of the shareholders and their percentage ratio of the capital.

9. List of all litigations, where the entrepreneur is or was sued, accused or the prodefendant.