215

ACT

of 11 March 2004

on the Protection of classified information and on the amendment and supplementing of certain acts

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

Article I

PART I
GENERAL PROVISIONS

Article 1
Subject of the Amendment

(1) This Act regulates the conditions for the protection of classified information, the rights and obligations of corporate entities and individuals pertaining to such protection, 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 established by this Act.

(2) This Act shall have no bearing upon the protection of secrets governed under specific regulation[1)].

[1)] For example Article 17 of the Commercial Code, Article 91 of Act no. 483/2001 Coll. on banks as amended by later legislation, Articles 23, 23a and 23b of Slovak National Council Act no. 511/1992 Coll. on the administration of taxes and charges and on changes to the system of territorial financial bodies, as amended by later legislation.

Article 2
Basic periods

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, unauthorised duplication, destruction, loss or theft (hereinafter referred to as “unauthorised handling”) and which may occur only in fields stipulated by the Government of the Slovak Republic through regulation,

(b) information shall be

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) a object shall be

1. a physical carrier with recorded information,
2. a product,
3. equipment,
4. real estate,

(d) detriment shall be understood as damage, or the threat of damage, to the interests of the Slovak Republic or to interests whose protection the Slovak Republic has been 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 categorised as extremely serious detriment, serious detriment, simple detriment and prejudicial to the interests of the Slovak Republic,

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

(f) an authorised person shall be a corporate entity or individual designated for acquaintance with classified information or whose authorisation for acquaintance with classified information ensues from the law,

(g) an unauthorised person shall be a individual not authorised for acquaintance with classified information, or not authorised for acquaintance with classified information beyond the designated scope applying to that person,

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

(i) technical device shall be 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) authorisation shall be the appointment of a state authority or corporate entity to perform an activity in certification,

(l) certifying authority shall be the execution of functions in connection with the issuance and verification of digital certificates of public keys used in asymmetrical encryption systems,

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

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

(o) an information protection encryption system shall be a set of devices for encryption protection of information together with the whole infrastructure for generating, distributing and liquidating encryption materials following the end of their validity,

(p) an information protection encryption device shall be equipment intended for the protection of information by encryption, and encryption materials,

(q) a building shall be a construction or otherwise delimited premises in which protected areas are situated,

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

(s) a mechanical prevention device is equipment or a system for preventing unauthorised persons from gaining access,

(t) technical safeguarding device shall be equipment or a system providing information on the state of the breaching of a building of protected areas.

Article 3
Security classification levels

(1) Classified information shall be categorised according to the security classification level into
(a) Top secret,
(b) Secret,
(c) Confidential,
(d) Restricted.

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

(3) The security classification level Top Secret shall be used to designate a classified information whose unauthorised 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 the field of defence, security, economic interests,

foreign policy or international relationships, and thereby could cause extremely serious damage to the interests of the Slovak Republic.

(4) The security classification level Secret shall be used to designate a classified information whose unauthorised handling could have the consequence of endangering the foreign policy standing, defence, security and interests of the state in the international and economic field, and thereby could cause serious damage to the interests of the Slovak Republic.

(5) The security classification level Confidential shall be used to designate a classified information whose unauthorised 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 thereby cause simple damage to the interests of the Slovak Republic.

(6) The security classification level Restricted shall be used to designate a classified information whose unauthorised handling could damage to the legally-protected interests of a corporate entity or a individual and that could be inconvenient to the interests of the Slovak Republic.

Article 4
Prohibition of the classification of certain information

(1) A classified information cannot be information on

(a) an 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 particulars, material provision and material advantages of public agents.

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

PART II
PROTECTION OF CLASSIFIED INFORMATION

TITLE I
FUNDAMENTAL PROVISIONS

Article 5
Classified information protection policy

(1) The policy of protecting classified information of the Slovak Republic is a set of aims, restrictions, requirements, rules and procedures that determine the process and development of the protection of classified information. The Classified Information Protection Policy of

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

the Slovak Republic shall be approved by the Government of the Slovak Republic at the proposal of the Authority Director.

(2) Ministries and other central bodies of the 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
Protection of classified information

(1) Classified information shall be protected from unauthorised persons and foreign powers by the method established in this Act, in regulations issued for its execution, and in separate regulations.[4]

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

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

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

(5) Administrative security is a system of measures whose objective is to ensure protection of classified information 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 serving for the protection of classified information from unauthorised persons and against unauthorised 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 under separate legislation[5] (hereinafter referred to as "a entrepreneur") for the protection of classified information submitted to, or originating at such a entrepreneur.

[3] Act no. 575/2001 Coll. on the organisation of government activity and on the organisation of the central state administration as amended.

[4] For example, the Criminal Act Act as amended, the Criminal Code as amended, Article 116(2) and Article 124 of the Civil Procedure Code as amended.

[5] For example Article 2 Commercial Code as amended.

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

(10) The Authority shall be empowered to issue generally binding legal regulations governing details on personnel security, administrative security, on physical security and building security, on the security of technical devices and on industrial security

Article 7
Change and extinction of security classification level

(1) If the need to protect information or an object containing classified information in a certain security classification level has lapsed, the originator of the classified information shall decide on a change or extinction of the security classification level. If a stipulated period for the security classification of information or an object containing classified information has elapsed, the originator of the classified information shall decide on a change or extinction of the security classification level.

(2) If a corporate entity in which a security classification level has been designated lapses and this corporate entity has no legal successor, or if the originator of the classified information is not known, the head of the state authority within whose competence the classified information falls shall decide on a change to or extinction of the security classification level.

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

Article 8
Duties of a head

(1) The responsibility for protecting classified information in a body of the state administration lies with the state 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 commission issued by the collective body to one of its members.

(2) The head shall in particular

(a) determine the fundamental scope of classified information, and unless he/she determines otherwise decide on the period of, change to, extinction of the security classification level according to Article 7(1),

---

[6)] Article 16 of Act no. 395/2002 Coll. on archives and registries and on the amendment of certain acts.

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

(c) ensure control of classified information within his/her jurisdiction and at the entrepreneurs to which classified information have been forwarded by the head,

(d) determine the positions whose execution allows authorised persons to be acquainted with classified information,

(e) provide for the execution of security clearance for security classification I,

(f) request the Authority to execute security clearance for security classification levels II to IV of persons proposed to be designated for acquaintance with classified information at the Confidential, Secret or Top Secret security classification levels,

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

(h) ensure the tuition of persons who are to be acquainted with classified information of the security classification degree Restricted that have been forwarded to the Slovak Republic by a foreign power; the tuition is performed according to the requirements of the foreign power,

(i) to notify the Authority in advance of the dissolution, fusion, merger, extinction or divesting of a state body or corporate entity at which classified information are stored,

(j) maintain registers and lists of authorised persons and of persons whose authorisation has expired,

(k) notify the Authority on changes in the scope of acquaintance with classified information that has occurred in the case of an authorised person, changes in the name and surname, marital status, residential address and state nationality of the authorised person, as well as on other facts reliably learnt and important for the inception of the authorisation pursuant to Article 10(1),

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

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

(n) notify the Authority in advance on the preparation and conclusion, with a foreign person or with the participation of a foreign person, of an international agreement or commercial contract a subject of which comprises classified information,

(o) perform other measures in the field of protecting classified information arising from this Act or from an international agreement,

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

(r) send to the Authority by the end of February, in electronic form or writing a list of all classified documents designated as Top Secret and Secret, that were filed in the protocols of documents of the respective security classification levels in the preceding 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 relates shall not be stated in the list.

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

Article 9
Specific workplace

(1) The head may, for the fulfilment of tasks arising from this Act and from its executive regulations, establish a specific workplace, or appoint an employee in writing (hereinafter referred to as "the security employee"), to perform these tasks in the extent defined by the head. If the quantity of tasks to be fulfilled or the complexity of the organisational structure requires so, the head may establish several specific workplaces or appoint in writing several security employees. Performance of a security employee or specific workplace function is contingent upon his/her holding a valid certificate, issued by the Authority, for acquaintance with classified information (hereinafter referred to as "the certificate") and confirmation, issued by the Authority, of having completed the security employee examination.

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

TITLE II
AUTHORISATION FOR ACQUAINTANCE WITH CLASSIFIED INFORMATION

Article 10
Conditions for the inception of an authorisation

(1) Unless specified otherwise in this Act, the authorisation for acquaintance with classified information for the security classification levels Top Secret, Secret, Confidential or Restricted materials 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 be acquainted with classified information and to undergo security clearance,

(e) being of integrity,

(f) guaranteeing through his/her conduct that he/she shall ensure the protection of classified information,

(g) being reliable as regards security,

(h) having a valid certificate, issued by the Authority, according to which he/she may be acquainted with classified information of the security classification level Top Secret, Secret or Confidential,

(i) having been accordingly designated,

(j) having signed the declaration of secrecy.

(2) The nominee shall continue to fulfil the conditions for the inception of the authorisation 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 be acquainted with classified information at the Restricted security classification level shall fulfil the conditions for the inception of the authorisation 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 21 years,

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

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

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

Article 12
Integrity of the nominee

(1) For the purposes of this Act a person shall not be considered to be of integrity if he/she has been lawfully convicted of an intentional criminal offence, unless he is viewed as having not been convicted.

(2) Even if a nominee is viewed as if having not been convicted, for the purposes of 2nd, 3rd, and 4th degree security clearance he/she shall not be considered to be a person of integrity if he/she has been lawfully convicted
(a) of a particularly serious felony,[7)] or
(b) of an intentional criminal offence of endangering classified information[8)] or of the criminal act of endangering confidential information or restricted information.[9)]

(3) The nominee shall prove his/her integrity through an extract from the Criminal Register ,[10)] which may not be more than three months' old.

[7)] Article 41 (2) of the Criminal Act.
[8)] Article 106 of the Criminal Act.
[9)] Article 173 of the Criminal Act
[10)] Act no. 311/1999 Coll. on the Criminal register as amended.

Article 13

Conduct of the nominee

A person who

(a) according to the conclusions of a medical examination is dependent on the use of alcoholic drinks or the use of other addictive substances,[11)]

(b) has been repeatedly sanctioned over the last five years for an offence in the field of the protection of classified information pursuant to Article 78.

shall not be deemed a person able, through his/her conduct, to guarantee the protection of classified information.

Article 14

Security Reliability of a nominee

(1) A person who has given false data in their personal questionnaire, in their security questionnaire, at a security interview, or who was assigned to and actively performed 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 up to 31 December 1989 – with the exception of persons who performed in these structures only an ancillary service or safeguarding function – or knowingly collaborated with these structures, or in the case of whom a security risk has been ascertained shall not be deemed reliable as regards security.

(2) A security risk shall be deemed to be

(a) activity performed against the interests of the Slovak Republic in the field of defence of the state, security of the state, international contacts, economic interests of the state, the 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 regulations, with consequences potentially endangering the interests of the Slovak Republic,

(c) a finding that the person

1. is or was a partner of spies, terrorists, saboteurs or of other persons having been reasonably suspected of such activities in the past,
2. is or was a member or supporter of any organisation striving by violent, subversive or other unlawful means to remove the democratic social order,
3. is under provable duress in consequence of a financial situation,
4. is provably dependent to the consumption of alcoholic drinks or other addictive substances,
5. is or was involved in any form of sexual conduct leading to blackmail or to constraint,
6. proved to be through his/her conduct or expression dishonesty, untrustworthiness in respect of the protection of classified information
7. seriously or repeatedly violated security regulations by trying without authorisation to

[11)] Artcle 89 (11) of the Criminal Act.

penetrate communication and information systems,

8. suffers or suffered any illness or mental or emotional condition that could cause substantial disorders in their reasoning and behaviour,
9. is under pressure from relatives or close friends who are open to exploitation by foreign intelligence and information services, terrorist groups, illegal organisations, risk groups or other similar individuals,
10. accepts unjustified payments, gifts or other benefits, or misuses his/her status and position in pursuit of the acquisition of unjustified benefits,
11. owns property whose value is not commensurate with his/her declared income and who is unable or unwilling to prove the lawful origin of such property,
12. completed study, a course or training of a security nature in the KGB University of Felix Edmundovič Dzeržinský of the former Union of Soviet Socialist Republics.

Article 15
Security clearance of the nominee

(1) Security clearance is performed in order to establish, whether or not a nominee fulfils the conditions stated in Article 10(1) for acquaintance with classified information

(2) According to the security classification level there shall be performed

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 III 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 specified otherwise by this Act, be

a) materials submitted by the nominee, namely
    1. completed personal questionnaire stated in Annex no. 2,
    2. curriculum vitae,
    3. a current extract from the Criminal Register in the case of 1st degree security clearance,
    4. written consent to the authorisation to be acquainted with classified information and to undergo of security clearance,
    5. completed security questionnaire stated in 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 Service 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 clearances performed at the place of residence by the Police Force, by the Slovak Information Service or Military Intelligence Service,

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

f) information from security clearances performed by the Police Force, Slovak Information Service or Military Intelligence Service on the security environment in which the nominee lives and moves and of the potential occurrence of security risks,

(2) The nominee shall submit the background material specified in paragraph 1(a) to his/her head; the nominee in his/her 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 his/her head in a sealed envelope so as to prevent him/her from familiarising him/herself with the contents.

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

(4) An application for the performance 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 the Council of the European Union or the European Commission. The nominee shall submit the background materials pursuant to paragraph 1(a) to the Authority. The provisions of Article 24(3) and Article 26(5) apply accordingly.

(5) The performance of a security clearance of a nominee may be requested also by a individual, a commission or other body, where a specific act provides for this.[12)]

(6) The nominee shall be entitled to provide the personal data required in accordance with Annex no. 3 Part A point 15. and Part B point 1.[13)]

Article 17
Performance of security clearances

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

(a) the head, where this concerns a 1st degree security classification,

(b) the Authority, where this concerns a 2nd, 3rd or 4th degree security classification.

[12)] For example 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 legal reversioners of the public prosecution as amended.
[13)] Article 7 (5) and Article 9 (1)(a) of Act no. 428/2002 Coll. on personal data protection.
[13a)] Constitutional Act No 254/2006 Coll. on the establishment and activity of the Committee of the National Council of the Slovak Republic for reviewing decisions of the National Security Authority.

Article 18

(1) The Slovak Information Service shall perform security clearances of all degrees, if the nominee in his/her relationship to the Slovak Information Service is an officer of it, an employee or applicant for admission into employment or a similar labour relationship, including a service relationship.

(2) The Military Intelligence Service shall perform security clearances of all degrees, if the nominee in his/her relationship to the Military Intelligence Service is an officer of it, an employee or applicant for admission into employment or a similar labour relationship, including a service relationship,

(3) The Military Intelligence Service shall perform security clearances also of 2nd, 3rd and 4th degrees, if the nominee is an employee of, or is in a similar labour relationship to, including service relationship to, the Ministry of Defence of the Slovak Republic (hereinafter referred to as the "Ministry of Defence"), or to organisations established or founded by the Ministry of Defence. It shall submit to the Authority the background materials pursuant to Article 16(1), together with an evaluation and proposal for the option of completing the security clearance pursuant to Article 26. Disputes as to the option of completing a security clearance between the Military Intelligence Service and the Authority shall be decided by the authority competent to decide on an appeal pursuant to Article 30 paragraph 3.

(4) The Police Force shall perform security clearance for all security classification levels of all degrees, if the nominee is a member of the Police Force or its employee, or is an applicant for acceptance into employment or into a similar labour relationship, including service relationship, and discharges or will discharge criminal intelligence duties,

(5) The Slovak Information Service, Military Intelligence Service and Police Force, in performing security clearance activities pursuant to paragraphs 1 through 4 are empowered to acquire the information stated in Article 16(1)(b) through (f) by their own activity.

Article 19

In performing security clearance activities of the 2nd, 3rd and 4th degree, the Authority, the Slovak Information Service, the Military Intelligence Service and the Police Force are empowered to request the provision of information as necessary for the execution of the security clearance and stated in Article 16(1)(b) through (f) including personal data [14)], from other state bodies, other corporate entities and individuals; these bodies and persons shall be obliged to comply with the request within the specified period and allow insight to the background materials on the basis of which the information for the security clearance purposes was provided. Legal persons or natural persons providing information on the nominee pursuant to Article 16 paragraph 1subparagraphs (c) to (f) must be additionally acquainted with the reason for which the nominee is being subject to security clearance.

[14)] Act no. 428/2002 Coll. on the protection of personal data.

Article 20
1st degree security clearance

The content of a 1st degree security clearance consists of an evaluation of the background materials specified in Article 16(1)(a) points 1 through 4.

Article 21
2nd degree security clearance

The content of a 2nd degree security clearance consists of an evaluation of the background materials specified in Article 16(1)(a) through (c).

Article 22
3rd degree security clearance

The content of a 3rd degree security clearance consists of an evaluation of the background materials specified in Article 16(1)(a) through (e).

Article 23
4th degree security clearance

The content of a 4th degree security clearance consists of an evaluation of the background materials specified in Article 16(1)(a) through (f).

Article 24
Commencement and discontinuance 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) points 1 through 5 to the Authority.

(2) The Authority shall discontinue a security clearance, if
(a) 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 shortcomings within the specified period,
(c) the nominee has died,
(d) it lacks competence to perform it or
(e) the Authority upon verifying new facts pursuant to Article 27 failed to find reasons for cancelling the validity of the certificate.

(3) The Authority shall discontinue the execution of security clearance also by written request of the head who requested its performance. In the request the head is obliged to state the reasons for discontinuing the security clearance.

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

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 impediment to the issuing of a certificate or represent a reason for the extinction of the certificate's validity. In the course of the security interview the nominee shall have the possibility to express his/her opinion as to the facts ascertained. A written record of the security interview shall be prepared 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 performed the security clearance, applying such methods as to avoid the violation of third-party rights and to not endanger any information source.

(3) The security interview may include a psycho-physiological examination of veracity, only if requested by the nominee. 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 identified factors that might be an obstacle for issue or cause for revocation of the certificate.

Article 26
Completion of a security clearance

(1) If the Authority, having established by security clearance that the nominee fulfils the conditions for the inception of an authorisation pursuant to Article 10(1), shall, instead of a written ruling, issue the certificate.

(2) If the Authority, having established by security clearance that the nominee does not fulfil the conditions for the inception of an authorisation pursuant to Article 10(1), shall issue a decision to this effect.

(3) The decision issued pursuant to paragraph 2 must state the provision under which the Authority decided that the nominee may not be 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 of appeal.

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

(5) The result of the security clearance shall be notified in writing to the head who requested its performance.

Article 27
Period for decision

(1) The Authority is obliged to decide on a security clearance of the
(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 stated in Article 16(1)(b) through (f) are obliged to submit to the Authority information on the security reliability of a nominee
(a) in the case of a 2nd degree security clearance within two months from the delivery of the request for the disclosure of information,
(b) in the case of a 3rd degree security clearance within three months from the delivery of the request for the disclosure of information,
(c) in the case of a 4th degree security clearance within five months from the delivery of the request for the 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 a further three months. The Authority is obliged to notify the nominee and the head who requested performance of the security clearance of the extension to the period, along with a statement of the reasons.

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

(5) The Authority shall interrupt a security clearance, if the nominee has been challenged 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 that of another similar labour relationship, including a service relationship.

Article 29
Annulment of a Certificate

The Authority is obliged upon the ascertaining of new facts during the validity of a certificate to verify whether the person fulfils the conditions for the inception of the authorisation pursuant to Article 10(1) and in the case of ascertaining that these the person does not fulfil these conditions, is obliged to annul the certificate. The provisions of articles 24 through 26 apply to such an annulment of a certificate accordingly.

Article 30
Procedure for reviewing decisions of the Authority

(1) A decision of the Authority pursuant to Article 26 paragraph 2, Article 29, Article 50 paragraphs 2 and 5 and Article 60 paragraph 7, with the exception of a decision of the Slovak Intelligence Service, Military Intelligence and Police Force, may be appealed by the person that has been served the decision 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. A appeal shall have a suspensive effect.

(2) The Authority may decide on an appeal alone if it allows an appeal in full. If the Authority does not take decision on an appeal alone, it shall submit it along with the opinion on the appeal lodged and other file documents related to the challenged 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 an appeal.

(3) The disputes concerning the method of completion of a security clearance between the Military Intelligence and the Authority according to Article 18 paragraph 3, and concerning an appeal according to paragraph 1 shall be decided by the Appellate Body, which is the Committee of the National Council of the Slovak Republic established by a special regulation. 13a) The procedure of the Appellate Body shall be determined by a special regulation. 13a)

(4) A decision of the Slovak Intelligence Service, Military Intelligence and Police Force pursuant to Article 26 paragraph 2 and Article 29 can be reviewed by court. The Supreme Court of the Slovak Republic shall have jurisdiction to review such decision.

(5) abolished from 30.12.2005

(6) abolished from 30.12.2005

(7) abolished from 30.12.2005
(8) abolished from 11.05.2006

(9) abolished from 11.05.2006

(10) abolished from 11.05.2006

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 be acquainted in the course of performing his/her function or discharging the duties of his/her position. A component of the designation is also acquaintance of the person with obligations in the protection of classified information and the possible consequences of their violation. Authorisation of the nominee for acquaintance with classified information arises through the signing of a record on the designation of the nominee for acquaintance with classified information, and through signing the non-disclosure declaration.

(2) Designation of a nominee meeting the conditions for the Restricted security classification level shall be performed by the head upon evaluation of a 1st degree security clearance. If the nominee fails to fulfil any of the conditions specified in Article 10(1), the head shall notify him/her of this fact in writing.

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

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

(5) Designation of an statutory body of a corporate entity as a person to which classified information are to be conferred shall be executed by the head of the state body that would confer the classified information; designation of the head of the entrepreneur to which classified information are to be conferred, or of the head of entrepreneur to be requested under Article 43 to create classified information, shall be executed by the Authority,

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

Article 32

(1) A record of the nominee’s designation for acquaintance with classified information of a specified security classification level, and his/her declaration of non-disclosure shall be attached to the document by which the employment or other similar labour 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 his/her declaration of non-disclosure within 30 days of that person’s designation.

Article 33
Personal security file

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

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

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

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

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

Article 34
Authorised persons having special status

(1) The following persons are authorised persons having special status within the scope of their respective positions pursuant to this Act
(a) the President of the Slovak Republic,
(b) a Deputy of the National Council of the Slovak Republic,
(c) a member of the Government of the Slovak Republic
(d) a 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 stated in paragraph 1 shall become authorised persons upon being elected or appointed to their office, or after pledging allegiance, if required under specific regulations.

(3) Unless specified otherwise in this Act, in a separate Act [15)] or in an international agreement binding upon the Slovak Republic, a security clearance shall not be performed on the persons stated in paragraph 1.

[14)] Act no. 428/2002 Coll. on the protection of personal data.

Article 35
Other authorised persons

(1) The chairman of a higher territorial unit and the mayor of a municipality may, in the scope required for the execution of his/her office, be acquainted with classified information at the Restricted level of security classification without undergoing security clearance. The head or security employee of a state body that confers the classified information shall advise the chairman of the higher territorial unit or municipality mayor of their obligations as to the protection of classified information and of the potential consequences of their violation, and shall ensure they sign a non-disclosure declaration. If a municipality mayor or chairman of a higher territorial unit is to be acquainted with classified information of the security classification level Confidential, Secret or Top Secret, he/she shall request the Authority to perform a security clearance of the respective degree on him/herself.

(2) An accused party, his/her defendant and other persons pursuant to specific legislation[16)], a witness at risk and a witness under protection[17)], a person acting in the interests of the authorities according to specific regulations[18)]and an agent[19)] may, upon signing the non-disclosure declaration and after being advised of their obligations as to the protection of classified information and of the potential consequences of their violation, may be acquainted with classified information in the scope necessary without fulfilling the conditions of Article 10. The advising of the person shall be performed by the official who familiarises him/her with the classified information, and this official shall keep a recorded to this effect in writing.

(3) A person who in proceedings before a state body is, on the basis of the consent of the head within whose competence the classified information falls, acquainted with classified information to the extent required for the purpose of the proceedings and once only, specifically an attorney, public notary, expert, interpreter or executor upon signing the non-disclosure declaration and after being advised of their obligations as to the protection of the classified information and on the potential consequences of their violation, shall be deemed an authorised person. This advising shall be performed by the person authorised to decide on calling this person to the proceedings; a record shall be prepared to this effect in writing.

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

[15)] For example Act no. 335/1991 Coll. as amended, Act no. 385/2000 Coll. as amended.
[16)] Article 201 (2) of the Code of Criminal Procedure.
[17)] Act no. 256/1998 Coll. on witness protection and on the amendment of certain acts in the wording of Act no. 490/2001 Coll.
[18)] 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 Service.
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 bodies of the state administration in customs in the wording of 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 in the wording of Act no. 422/2002 Coll.
[19)] Article 88b of the Code of Criminal Procedure.

Article 36

(1) A foreign national who is the citizen of a country that has concluded an agreement on the protection of classified information exchanged with the Slovak Republic may be acquainted with classified information.

(2) A foreign national may be acquainted with classified information of the security classification levels Confidential through to Top Secret only on the basis of the written consent of the head of the state body within whose competence the classified information fall and only upon the prior issuance of a certificate by the Authority, unless an international agreement states otherwise.

(3) The Authority shall issue a certificate pursuant to paragraph 2 to a foreign national only after obtaining an opinion as to his/her security reliability from the competent body of his/her home state.

(4) The head specified in paragraph 2 shall advise the foreign national of the obligations under this Act and of the potential consequences of their violation, and ensure the person signs a non-disclosure declaration, unless an international agreement states 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 the state administration within whose competence the classified information falls, and on the basis of consenting opinions of the Ministry of Foreign Affairs of the Slovak Republic, the Ministry of Interior of the Slovak Republic, the Slovak Information Service, the Military Intelligence Service and of the Authority.

(6) Paragraphs 1 to 5 shall apply accordingly to acquaintance with classified information in the case of entrepreneurs of a foreign state,

Article 37

The persons specified in Article 36(1) may be acquainted with classified information of the security classification level Restricted only with consent of the state body within whose competence the classified information fall; 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 states otherwise.

Article 38
Obligations of authorised persons

An authorised person is obliged to

(a) keep secret on information and objects containing classified information, while they are classified, before unauthorised persons and foreign powers, including after the lapsing of the authorisation to be acquainted with classified information,

(b) comply with generally binding legal regulations governing the protection of classified information,

(c) notify the head without delay of any unauthorised handling of classified information and any interest of unauthorised persons in classified information, and to cooperate with the Authority as regards clarifying the causes of the unauthorised handling of the classified

information; authorised persons having special status shall notify the Authority of any unauthorised handling of classified information and any interest of unauthorised persons in classified information,

(d) notify the head without delay of a change of name and surname, marital status, residence, state nationality and integrity,

(e) notify the head without delay of any fact potentially influencing his/her authorisation to be acquainted with classified information, and of any fact potentially influencing such authorisation of another authorised person.

Article 39
Obligations of unauthorised persons

(1) An unauthorised person who obtains any classified information or classified object is obliged to surrender it without delay to the Authority or to a unit of the Police Force; at the request of this person surrendering the classified information or classified object, the recipient shall issue a document on its receipt.

(2) An unauthorised 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 keep secret on the materials with which he/she has become acquainted.

Article 40
Release from the non-disclosure obligation

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

(2) The President of the Slovak Republic, a 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 Office, a judge of the Constitutional Court of the Slovak Republic may be released, for the purpose specified in paragraph 1, from the obligation to not disclose classified information with which they have become acquainted while discharging 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 specified in paragraph 1, from the obligation to not disclose classified information with which he/she has become acquainted while discharging his/her functions, by the President of the Slovak Republic,

(4) A judge may be released, for the purpose specified in paragraph 1, from the obligation to not disclose classified information with which he/she has become acquainted with while discharging his/her functions, by the Judicial Council of the Slovak Republic.

(5) Members of the Government may be released, for the purpose specified in paragraph 1, from the obligation to not disclose classified information, by the Prime Minister of the Slovak Republic. Heads of other central bodies of the state administration and senior state

officials may be released, for the purpose specified in paragraph 1, from the obligation to not 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 to not disclose classified information, specifying the purpose, scope and duration from which the release is valid. The head shall send one copy of the record without delay to the Authority; this shall not apply to the Slovak Information Service, the Military Intelligence Service and to the Police Force of the Slovak Republic in connection with discharging criminal intelligence duties.

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

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

Article 41
Lapsing of a designation

(1) The designation of a person to be acquainted with classified information shall lapse through the

(a) lapsing of the validity of their certificate,

(b) termination of the performance of their position,

(c) termination of their employment or similar labour relationship, or through the fulfilment of his/her contractual commitment,

(d) annulment of the certificate pursuant to Article 29 within the period of reviewing a decision of the Authority pursuant to Article 30,

(e) extinction, by the head, of the designation to be acquainted with classified information,

(f) finishing of compulsory military service or

(g) declaration of the person’s death.

(2) The head shall prepare a written record on the lapsing expiry of a designation to be acquainted with classified information, and take measures toward their protection.

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

Article 42
Keeping of records

(1) The Authority shall maintain records on authorised persons cleared for Top Secret, Secret and Confidential security classification levels, along with records on persons whose authorisation has lapsed; this shall not apply to authorised persons who are or have been members or employees of the Slovak Information Service, Military Intelligence Service, members or employees of the Police Force of the Slovak Republic who discharge criminal intelligence duties and are maintained in their records.

(2) Heads shall keep records on authorised persons cleared for the Restricted security classification level, records on persons whose authorisation has lapsed, and a list of authorised persons cleared for the Top Secret, Secret and Confidential security classification levels, and a list of persons whose clearance has lapsed.

(3) Records of authorised persons whose authorisation to be acquainted with classified information at the security clearance levels Top Secret and Secret has lapsed shall be maintained for twenty years from the lapsing of this authorisation.

(4) Records of authorised persons whose authorisation to be acquainted with classified information at the security clearance level Confidential has lapsed shall be maintained for three years from the lapsing of this authorisation.

(5) Records of authorised persons whose authorisation to be acquainted with classified information at the security clearance level Restricted has lapsed shall be maintained for one year from such the lapsing of this authorisation.

(6) The Authority, the Slovak Information Service, the Military Intelligence Service, the Police Force of the Slovak Republic in discharging duties in the field of criminal intelligence and heads are obliged under a specific regulation[14)] to ensure the protection of data in their records against unauthorised handling.

(7) Upon the elapsing of the deadlines specified in paragraphs 3 through 5 the Authority, the Slovak Information Service, the Military Intelligence Service, the Police Force of the Slovak Republic discharging duties in the field of criminal intelligence and the head shall destroy data kept in archives for the purpose of protecting classified information.

(8) The records pursuant to paragraph 1 of the Authority, of the Slovak Information Service, of the Military Intelligence Service, and of the Police of the Slovak Republic in discharging duties in the field of criminal intelligence are records maintained in connection with protecting classified information. These records shall not be subject to registration of information systems in connection with the protection of personal data[14)].

TITLE III

ENTREPRENEURS

Article 43
Industrial security

If the assumption is justified that a state body will require a entrepreneur to create classified information, or if it will be necessary to confer classified information from a state body to a entrepreneur (hereinafter referred to as the “transfer of classified information”), the

entrepreneur is obliged to request the Authority for issuance of an industrial security certificate.

Article 44
Transfer of classified information

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

(2) The contract pursuant to paragraph 1 shall contain a specification of the transferred classified information, their security classification level, the period for which the classified information will be transferred, a list of persons, the scope of their authorisation to be acquainted with the classified information, the scope of activities involving the classified information, the range of control measures, the obligation to notify of the extinction of the entrepreneur or changes influencing the protection of the classified information, the transfer of the classified information to a different entrepreneur, as well as obligations of the entrepreneur upon the lapsing of the industrial security certificate's validity.

(3) The state body transferring the classified information is empowered to control compliance with their protection also in the entrepreneur to which it transferred the classified information. The results of the control 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 empowered to perform immediate measures for ensuring the protection of the transferred classified information, including seizure of the classified information.

Article 45
Security clearance of an entrepreneur

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

(2) The Authority shall perform 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) a written justification for the request,
(b) the level of security classification and the period of validity for which the certificate is requested,
(c) security project of the entrepreneur,
(d) a security questionnaire for the entrepreneur, completed pursuant to Annex No. 3,
(e) documents or their authenticated copies confirming the veracity of the data in the entrepreneur security questionnaire.
(f) a request for the performance of 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)If the request has deficiencies due to which it is not possible to commence the security clearance, the Authority shall interrupt the security clearance and challenge the entrepreneur to remove them within a set 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 discontinued.

(6) The Authority shall interrupt the security clearance of an entrepreneur, if the entrepreneur changed or added during the performance of the security clearance the statutory body whom the Authority did not issue a certificate according to Article 26, till the date necessary for the performance of security clearance of the statutory body. The Authority shall interrupt the security clearance, also if there is an ongoing proceeding in which the question which might be of significance to completion of security clearance is solved, until the completion of the proceeding.

(7) The Authority shall discontinue performance of an entrepreneur's security clearance also on the basis of its written request. In this request the entrepreneur is obliged to state the reasons for suspension of the security clearance.

(8) The security project of an entrepreneur is the project of a system for the protection of classified information at the entrepreneur. The security project of an entrepreneur comprises mainly a definition of the security policy and method of its implementation in the field of personal 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 be acquainted with the classified information.

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

(10) An entrepreneur is obliged, for the purpose of ascertaining its industrial security, to allow members 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 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 certificate.

(12) The Authority is empowered to issue generally binding legal regulations, establishing the particulars of the entrepreneur's security project.

Article 46
Conditions for issuing an industrial security certificate

An industrial security certificate may only be issued to a entrepreneur that is
(a) capable of protecting classified information,
(b) economically stable,
(c) reliable as regards security.

Article 47

An entrepreneur lacking conditions for protecting classified information under this Act shall not be considered capable of protecting classified information.

Article 48

An entrepreneur
(a) that is in liquidation,
(b) against which bankruptcy has been declared,
(c) on whose assets settlement has been permitted,
(d) that fails to meet financial obligations toward the state or
(e) repeatedly fails to meet financial obligations toward other individuals or corporate entities.

shall not be deemed an economically stable entrepreneur.

Article 49

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

(2) A security risk shall be deemed to be
(a) action against the interests of the Slovak Republic in the field of state defence, state security, international relations, economic interests of the state, functioning of a state body, or against interests that the Slovak Republic has undertaken to protect,
(b) a 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 from the field of organised crime,
(d) corrupt conduct of the entrepreneur,
(e) staffing instability in managing positions or bodies of the entrepreneur or
(f) the annulment of the entrepreneur's certificate.

Article 50
The industrial security certificate

(1) Where the security clearance finds that the entrepreneur fulfils the conditions pursuant to Article 46, the Authority shall issue an industrial security certificate.

(2) Where the security clearance ascertains that the entrepreneur does not fulfil the conditions stated in Article 46, the Authority shall issue a decision to this effect.

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

(4) The entrepreneur is authorised to be acquainted with classified information up to the security classification level specified in the industrial security certificate issued to it.

(5) If the Authority finds that the entrepreneur has ceased to fulfil any of the conditions of industrial security specified in Article 46, or has grossly or repeatedly violated its obligations in the field of protection of classified information, the Authority shall annul the entrepreneur's industrial security certificate.

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

(7) The Authority shall maintain a list of entrepreneurs to which industrial security certificates have been issued, and a list of entrepreneurs whose industrial security certificates have lapsed.

Article 51
Period for issuing an industrial security 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) The Slovak Information Service, Military Intelligence Service, 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 a further 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
Extinction of the validity of the industrial security certificate

(1) The validity of the industrial security certificate shall extinct through
(a) the elapsing of the period of the industrial security certificate's validity,
(b) extinction of the entrepreneur or
(c) a notification made pursuant to Article 50(5).

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

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

(4) In the case of the validity of the industrial security certificate lapsing pursuant to paragraph 1, its head shall ensure the protection of the classified information against unauthorised 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 method, 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 shall not apply to ensuring the placement of special devices, performed in accordance with specific regulations[20)]

(6) The Authority is empowered to issue generally binding legal regulations, establishing 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 the protection of classified information designated as of the security classification level Confidential and higher are subject to certification by the Authority.

(2) The following types of certifications exist

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”),

[20)] For example, Article 88, 88a, 88c and 88d of the Code of Criminal Procedure, 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.

(3) The manufacturer, importer or distributor shall apply to the Authority for issuance of a type certificate.

(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 connected with certification shall be covered by the applicant for certification.

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

(11) The Authority is empowered to issue generally binding legal regulations, establishing 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 so as to ensure the protection of classified information.

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

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

(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 five years at most for the security classification levels Top Secret and Secret and seven years at most 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 discontinue use of the technical devices. The filing of a remonstrance 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 Defence of the Slovak Republic or the Slovak Information Service shall be discontinu ed by their heads at the proposal of the Authority.

(8) The use of the technical device may be renewed only with the written consent of the Authority and only after elimination of the deficiencies that led to the suspension of use.

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

§ 56
Certification of technical devices

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

(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 levels, and its validity is contingent upon compliance with the conditions and rules of use defined 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 at most five years for the security classification levels Top Secret and Secret, and seven years at most for the security classification levels Confidential and Restricted.

(6) Expenses connected with certification shall be covered by the applicant for certification.

(7) The Authority is empowered to issue generally binding legal regulations, establishing 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 performed by the Authority; this shall not apply to system devices used within the competence of the Slovak Information Service and of the Military Intelligence Service.

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

(a) operating systems, their individual versions and modifications,

(b) database systems,

(c) products for the administration and operation of computer networks,

(d) products for the administration and operation of the electronic mail,

(e) firewalls and special system security products,

(f) other functionally specialised system products intended for the creation, processing, transfer or storage of classified information.

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

Article 58
Security project for technical devices

(1) The security project for technical devices determines the scope and method 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) the security aim,

(b) a description of the technical devices**,**

(c) an analysis of the protection of classified information from the aspect of loss, violation of secrecy, accessibility, integrity and authenticity of the classified information, classification of the main threats to the classified information, possible counter-measures against individual threats from the aspect of prevention, detection and elimination,

(d) use of security standards and the determination of other methods and means used for protecting classified information,

(e) the specification of threats secured by protective measures and their effectiveness,

(f) the specification of threats not secured by protective measures,

(g) guidelines for emergency planning and resumption of the 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 empowered to issue generally binding legal regulations, establishing the particulars of processing the security project for technical devices and on the issuing and use of security standards.

Second Section
Authorisation

Article 59

(1) Consent to the authorisation 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. There shall be no legal claim to authorisation.

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

(3) The Authority may issue consent to an authorisation on 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 for performing the certification,

(b) has the premises and technical equipment necessary for performing the certification,

(c) is organisationally capable of ensuring impartiality in the performance of certification activities,

(d) has taken out professional liability insurance,

(e) is a person authorised or accredited in accordance with specific legislation.[22)2)2)2)]

(4) In its consent to the authorisation of a state body or to the authorisation of a entrepreneur the Authority shall specify 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 authorised state body or who are the statutory body of the authorised entrepreneur, or a members of such a statutory body, specifying the manner and scope of their acting on behalf of the authorised state body or of the authorised entrepreneur,

(e) scope and conditions of activities to be performed,

(f) period for which the authorisation is valid.

[22)] For example, Act no. 264/1999 Coll., Act no. 90/1998 Coll. on building products as amended.

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

(a) perform technical examinations objectively and at the scientific and technological level representing the state of the art at the time the examinations are performed,

(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 authorisation,

(6) The authorised state body or authorised entrepreneur is empowered to

(a) examine, in the performance of its activity, the technical, production and other documentation relating to the certified device,

(b) use on documents issued under this Act a stamp registered by the Authority,

(c) claim reimbursement of its expenses in connection with the certification from the applicant for certification.

(7) The Authority is empowered to control, whether state bodies or entrepreneurs authorised by the Authority comply with the provisions of this Act and with the conditions specified in the consent to the authorisation.

(8) If an authorised state body or authorised entrepreneur has ceased to fulfil the conditions established by this Act and the conditions specified in the consent to the authorisation, or if it has violated legal regulations relating to the scope of its commission or the content of activity, or if an authorised state body or an authorised entrepreneur has applied for such an amendment or extinction, the Authority shall amend or cancel its consent to the authorisation. Should an authorised state body or authorised entrepreneur apply for extinction of its authorisation, it must do so at least six months before the date proposed for extinction of the authorisation.

(9) An authorised state body or authorised entrepreneur may apply for an extension to the validity of the consent to the authorisation at least six months before expiry of the validity of the consent to the authorisation. The Authority shall extend the validity of the consent to the authorisation, if it is established that all the conditions specified therein and in this Act remain fulfilled by the authorised state body, or by the authorised entrepreneur.

TITLE VI
PROTECTION OF FOREIGN INFORMATION

Article 60
Exchange of classified information

(1) Classified information protected by a foreign power and provided to the Slovak Republic shall be protected under this Act, if so ruled 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 specified otherwise herein, classified information of the Slovak Republic may be provided 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 organisation 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, unless such provision would be at variance with other international agreements binding upon the Slovak Republic.

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

(4) Decisions on the provision of classified information by a corporate entity of the Slovak Republic to a foreign person shall be made by the Authority. The Authority shall, before such provision, request an opinion from the Ministry of Foreign Affairs of the Slovak Republic, the Slovak Information Service, the Ministry of Defence, the Ministry of the Interior, and the central body of the state administration within whose competence the classified information falls; these bodies are obliged to comply with the request. The Authority shall also request an opinion from the competent body of the state in which the foreign person is registered.

(5) The provision and acceptance of classified information shall be performed by means of the central register managed by the Authority, unless stipulated otherwise by an international agreement binding upon the Slovak Republic.

(6) In compliance with international agreements binding upon the Slovak Republic, the Authority and the competent authority of the other state are empowered to control protection of the mutually provided classified information.

(7) The Authority shall perform security clearance of the individuals who are to be acquainted with the classified information in connection with discharging their duties under 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 certificates. If among such individuals there is a person already subjected to security clearance pursuant to Article 18, the Authority shall issue the security clearance certificate on the basis of an assessment of his/her personal security file.

(8) Paragraphs 3 through 6 shall not apply to the provision 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 other states in the framework of cooperation executed under specific legislation[23)] in such cases consent to the provision of classified information must be made, and recorded, by the heads of the intelligence services or by the Minister of Interior of the Slovak Republic.

Article 61
Registers of classified information and international cooperation

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

(2) State bodies and corporate entities providing and accepting 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 execute management and coordination of encryption protection of information in the field of 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 defence 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) The prohibition of photographing, filming or making other records, and exceptions from the prohibition shall be decided upon by the central body of the state administration within whose competence the classified information falls.

Article 64
Aerial photographing and the performance of geodesic and cartographic works

(1) Aerial photographing of the territory of the Slovak Republic and the performance of geodesic and cartographic works (hereinafter referred to as "aerial photographing") is performed by the Ministry of Defence of the Slovak Republic[24)]. With the consent of the aforesaid Ministry aerial photographing may also be performed by a entrepreneur holding a valid security clearance certificate.

[23)] For example, 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.

[24)] Article 4 (4) of Act no. 215/1995 Coll. on geodesy and cartography.

(2) A entrepreneur specified in paragraph 1 may perform aerial photographing only in the case that it holds an aerial work permit[25)], or may commission another entrepreneur holding an aerial work permit to perform aerial photographing, unless specified otherwise by an international agreement[26)] binding upon the Slovak Republic.

(3) The application for an aerial photographing permit shall be submitted to the Ministry of Defence of the Slovak Republic. The application shall contain the particulars specified in a specific regulation [27)].

(4) The Applicant shall, within one month, notify the Authority that it has acquired aerial photography material, and submit it to the Ministry of Defence of the Slovak Republic for assessing the security classification level of the photographic material. Until such assessment of the aerial photographic, the material shall be handled as classified information.

PART III
ENCRYPTION PROTECTION OF INFORMATION

Article 65
Central Encryption Office

(1) The Central Encryption Office shall coordinate and control the activity of central bodies of the state administration in the field of the encryption protection of information. In relation to the intelligence services of the Slovak Republic the controlling activities of the Central Encryption Office are limited to the level of departmental encryption offices and their equivalent encryption bodies.

(2) The Central Encryption Office is empowered to request information from central bodies of the state administration as required for discharging its duties.

(3) Unless excluded by this Act or by a separate regulation, employees of the Central Encryption Office shall be empowered in connection with controlling the security of systems and devices used for the encryption protection of information to enter workplaces of encryption offices.

(4) In the case of detecting serious deficiencies in the field of encryption protection of information the Central Encryption Office may, by decision, discontinue the operation of a system or device used for the encryption protection of information. Filing of a remonstrance [28)] against the decision shall have no suspensive effect.

(5) The suspension of the operation of a system or device used for the encryption protection of information of the Ministry of Interior of the Slovak Republic, the Ministry of

---

[25)] Article 44 of Act no. 143/1998 Coll. on civil aviation (the Aviation Act) and on the amendment of certain acts in the wording of Act no. 37/2002 Coll.
[26)] For example, the Open Skies Agreement (notice no. 374/2002 Coll.).
[27)] Article11 Decree no.177/1996 Coll. on the performance of geodetic and cartographic activities for the needs of state defence.
[28)] Article 61of Act no. 71/1967 Coll. on administrative action (the Administrative Code).

Defence and the Slovak Information Service shall be executed by the head at proposal of the Central Encryption Office.

(6) The operation of the system or device used for the encryption protection of information may be restored only with written consent of the Central Encryption Office and after removal of the deficiencies that led to the suspension the operation.

Article 66
Departmental Encryption Offices

(1) The head of a central body of the state administration is empowered to establish, with prior consent of the Central Encryption Office, a departmental encryption office as a specialised workplace for ensuring the encryption protection of information within the competence of that central body of the state administration.

(2) A departmental encryption office shall report directly to the head of the central body of the state administration.

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

(a) is responsible for the encryption protection of information within his/her competence,

(b) determines the scope of duties of the departmental encryption office within his/her competence and of an equivalent encryption office,

(c) approves the operation of certified systems and devices for the encryption protection of information,

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

(e) discontinues the operation of systems and devices for the encryption protection of information in the case of detecting deficiencies in the field of the encryption protection of information, and informs the Central Encryption Office of the suspension.

Article 67
Certifying authority

(1) The Central Encryption Office executes the function of the certifying authority for the protection of classified information.

(2) In executing the function pursuant to paragraph 1, the Central Encryption Office shall

(a) issue digital certificates,

(b) manage digital certificates,

(c) provide services connected with digital certificates,

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

Article 68
Professional qualification

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

(2) The employee specified in paragraph 1 shall be issued a certificate by the head of the central body of the state administration, authorising him/her for work in the specified field of the encryption protection of information.

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

Article 69

The Authority is empowered to issue generally binding legal regulations, establishing the particulars of certification and operational approval of systems and devices for the encryption protection of information, their use, implementation, transport and registration, use of encryption materials, maintaining files on employees in the field of the encryption protection of information and verification of their professional qualification, and details on establishing departmental encryption offices or equivalent encryption offices.

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

Article 70
Competences of the Authority, status, obligations and powers of members of the Authority

(1) The Authority shall, in the field of

(a) the protection of classified information

1. elaborate a classified information protection policy and analyses of the state and level of work in this field,
2. exercise control over the protection of classified information,
3. ensure the execution of security clearance for nominees and for 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 cancel a certificate on a nominee,
5. execute training of security employees,
6. issue and cancel an industrial security certificate of a entrepreneur
7. certify technical devices, system devices, mechanical prevention devices and technical safeguarding devices, and issue security standards,
8. authorise state bodies and entrepreneurs to certify technical devices, mechanical prevention devices and technical safeguarding devices,
9. issue security standards,
10. execute expert activity,
11. maintain records relating to the protection of classified information,
12. issue methodological guidance for activity in the field of the protection of classified information,
13. ensure tasks related to the protection of classified information in the case of the extinction of state bodies and corporate entities without a legal successor,
14. execute and ensure research and development in the field of information technology security,

(b) the protection of foreign information

1. execute tasks in the field of the protection of classified information within the scope established by international agreements,
2. set principles on the exchange and protection of classified information in accordance with international agreements under preparation or those in force,
3. control compliance with and performance of international agreements on the exchange of classified information,

4. give its opinion on nominees according to international agreements and issue the respective certificates,
5. discharge duties concerning the central register for the exchange of classified information,
6. maintain records relating to the exchange of classified information,

(c) the encryption protection of information

1. fulfil the function of the Central Encryption Office of the Slovak Republic,
2. elaborate the policy on the development of information encryption protection,
3. lay down principles on the information encryption protection,
4. certify, verify and recognise foreign certificates and approve for operation methods, systems and devices of information encryption protection for the protection of classified information at the Top Secret and Secret security classification levels, unless laid down otherwise herein,
5. recommend or certify or verify and recognise foreign certificates and approve for operation systems and devices of the encryption protection of information for protecting classified information at the Confidential and Restricted security classification levels,
6. execute security controls over the encryption protection of information,
7. determine the conditions for the selection, professional preparation of employees and the conditions for the issuance and revocation of work certificates,
8. determine the scope and method of the use of an information system of information encryption protection,
9. execute and ensure research and development in the field of cryptography, and research, development and production of devices for the encryption protection of information,
10. determine the method, scope and conditions for the administration of systems for the information encryption protection and of the production of encryption materials for systems and devices of the encryption protection of information,
11. execute expert activity,
12. maintain records relating to the encryption protection of information,
13. fulfil the function of the sponsor of the government and foreign linkage,
14. fulfil the function of the sponsor of securing devices of information encryption protection,
15. issue security standards for the encryption protection of information and for protection from undesirable electromagnetic radiation of technical devices and devices of the encryption protection of information,

(d) internal protection, acquire, gather, analyse and verify information on the security risks relating to the scope of activities of the Authority and its members and employees.

(2) The Authority, in discharging its tasks under paragraph 1(d), is entitled to request from state bodies, corporate entities and individuals assistance, background documentation and information that may contribute to the prevention and elimination of

security risks. No person may be coerced to provide assistance, background documentation or information.

(3) The Authority may discharge its tasks set out in paragraph 1 also outside the territory of the Slovak Republic, if arising from international agreements binding upon the Slovak Republic or on the basis of the agreement of the parties involved. Decisions on the dispatching of members 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 organisations.

(5) The Authority shall discharge its tasks under this Act through its members who are in a service relationship pursuant to a specific regulation[1].

(6) A member of the Authority shall manifest his/her membership of the Authority by a service pass stating a registration number, and by the verbal statement: "National Security Authority".

(7) A member of the Authority is obliged, in discharging his/her tasks, to be mindful of the honour, respect and dignity of persons, including themselves, and shall take care to prevent harm or other detriment to persons in connection with his/her activities.

(8) A member of the Authority shall be authorised by the Director to carry a firearm and use it within the limits of the law for averting an attack directed against him/her or directly threatening him/her, or an attack against the life of another person, provided that it cannot be averted otherwise.

(9) A member shall, prior to using a firearm, be obliged to challenge the person to desist from the unlawful activity and warn the person that the firearm will be used. Prior to using the firearm the member shall be obliged to fire a warning shot. The member may waive the obligation to challenge 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 a member shall be obliged to proceed with the necessary caution, in particular in order to prevent any threat to the life of other persons and to as far as possible spare the life of the person against whom the firearm is used. Members shall be obliged to report the use of a firearm to his/her superior.

(11) Tasks of the Authority may also be discharged with the participation of employees in a labour relationship, the particulars of which are governed by specific regulations[2].

[1] Act no. 73/1998 Coll. on state service of members of the Police Force, Slovak Information Service, Prison and Judiciary Guard Corps of the Slovak Republic and the Railways Police, as amended.
[2] The Labour Code.

Article 71
Director of the Authority

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

(2) The Director of the Authority, if he/she fulfils the conditions of Article 10, shall be appointed and recalled by the National Council of the Slovak Republic at the proposal of the Government of the Slovak Republic. The period of office of the Director of the Authority shall be seven years, commencing from the date of his/her appointment to the office of the Director of the Authority.

(3) The same person may be appointed Director of the Authority for at most two periods of office.

(4) The office of the Director of the Authority is incompatible with the discharge of an office in another public authority, with employment or a similar labour relationship, with the conduct of business activities, with membership in a managing or controlling body of a corporate entity conducting business activities, or with any other economic or gainful activities, except for the administration of his/her own property, scientific, pedagogical, journalistic, literary or arts activities.

(5) The discharge of the office of the Director of the Authority shall periodinate through the elapsing of the periodof office. Prior to the elapsing of the periodof office, the office of the Director of authority periodinates only through

(a) resignation from the position,

(b) recall from the position,

d) death or presumption of death of the Director of the Authority.

(6) The Director of the Authority may resign from this position through a written notification to the Chairman of the National Council of the Slovak Republic. In such a case, the discharge of the office shall periodinate through the elapsing of the calendar month following the month in which the notification of the Director of the Authority on the resignation of the position was received by the Chairman of the National Council of the Slovak Republic, unless another agreement concerning the date of periodination of the discharge of the office of the Director of the Authority between the Chairman of the National Council of the Slovak Republic has been reached.

(7) The National Council of the Slovak Republic may recall the Director of the Authority from the position on the basis of a proposal of 30 deputies, or at the proposal of the Governement, or if the Director of the Authority

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

(b) has started to perform a position or conduct activities incompatible with the office,

(c) has been convicted of perpetrating a criminal offence by legally valid court decision,

(d) has been lawfully incapacitated, or his/her 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 discharge his/her office for health reasons according to a medical opinion, decision of a body of the national health authority or a social care body,

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

(i) lost the authorisation to be acquainted with classified information under Articles 28 and 29.

(8) The Director of the Authority shall be recalled from the office from the date following the day when the decision of the Chairman of the National Council of the Slovak Republic was delivered to the Director of the Authority, recalling him/her from office.

(9) The Director of the Authority shall have six weeks of holiday in a calendar year. For holiday time include Director of the Authority salary.

(10) The Director of the Authority shall prove his identity during his official activities by a service pass issued by the Authority.

(11) All documents related to the function of the Director of the Authority shall be filed to his personal file maintained by the Authority. The personal file is kept for the period of 50 years, after the accomplishment of his function.

(12) The provisions of Articles 45, 54, 59 through 62, 68, 70, 115 through 117 of Act no. 400/2009 coll. on state service as amended and Articles 116 (2) and (3), 136 (1), 137 (1), (4) and (5), 138, 141, 144, 177 through 222 of Labor Code shall be applied mutatis mutandis, while executing the Director of the Authority.

Article 71 (a)

Emoluments, material benefits and lump sum compensations of the Director of the Authority.

(1) The Director of the Authority is featured monthly salary of the monthly salary of a member 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 after his term of office shall have a compensation of three times the monthly salary of his term. Functional salary shall be rounded up to the nearest Euro.

(2) The Director of the Authority while executing has a right to free

a) use of an official vehicle assigned with or without a driver to perform a function, or in connection with,

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 have a monthly lump sum compensation of 54% of the salary to cover the necessary expenses for personal services and other expenses associated with his function. The flat-rate compensation is determined by a fixed amount rounded up to the nearest euro.

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

(5) For the purposes of health insurance, hospital insurance and pension insurance, the Director of the Authority is considered an employee in employment.

Article 72
Control of the Authority by the National Council of the Slovak Republic

(1) Control 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 specific control body (hereinafter referred to as the "Control Body") composed of deputies.

(2) Members of the Control Body are entitled to enter, in the company of a member of the Authority, protected areas of the Authority and familiarise themselves with classified information relating to the activities of the Authority, unless at variance with an international agreement binding upon the Slovak Republic.

(3) Should the Control Body, in discharging its powers, find any violation of this Act 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 laid down otherwise herein, a specific regulation[3] shall apply to the proceedings of the Control Body and to its rights and the obligations of its members accordingly.

Article 73

(1) The National Council of the Slovak Republic shall elect at the beginning of each electoral periodthe members of the Control Body and determine the number of its members, composition and method of this body's work.

(2) Should a deputy, a member of the Control Body, leave the club of deputies, he/she shall lose membership in this the Control Body. For this member, the club of deputies shall propose a new member.

(3) Meetings of the Control Body are not public. The Control Body shall meet at least once a quarterly. In negotiating it shall proceed according to its rules of procedure. Every member of the Control Body may requrest its convocation.

(4) Following the periodination of an electoral periodof the National Council of the Slovak Republic the Control Body shall perform its activity until the National Council of the Slovak Republic elects a new Control Body in the new electoral period.

[3] National Council of the Slovak Republic Act no. 350/1996 Coll. on rules of procedure of the National Council of the Slovak Republic, as amended.

Article 74

(1) Notification shall be given of facts of which members of the Control Body learn in discharging their functions only in the scope necessary for achieving the purpose of control pursuant to this Act.

(2) Members of the Control Body shall be obliged to keep secret on facts of which they have learnt in discharging their position. The obligation to keep secret shall also continue following the periodination of their position as member of the Control Body, and only the National Council of the Slovak Republic may release them from this obligation.

Article 75
The Slovak Information Service and the Military Intelligence Service

(1) The Slovak Information Service and the Military Intelligence Service shall

(a) perform security clearances of nominees within their respective competences pursuant to Article 19,

(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 perform security clearance, 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 clearances to the Authority,

(d) at the request of the Authority perform security clearance, within the scope of their respective competences, on the security of the environment in which the nominee lives, the occurrence of potential security risks and provide the information from these clearances to the Authority,

(e) at the request of the Authority provide information required to determine the industrial security of entrepreneurs,

(f) approve the operation of and certify technical devices used exclusively within their respective competences,

(g) maintain records relating to the protection of classified information,

(h) maintain registers of classified information, provided and accepted within the framework of international cooperation,

(i) carry out training of their security employees.

(2) The Slovak Information Service and the Military Intelligence Service are empowered, in discharging their tasks under paragraph 1, to

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

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

(c) maintain in their records data acquired while discharging their tasks under this Act.

(3) The Slovak Information Service and the Military Intelligence Service are empowered to apply information-operational devices under a specific regulation[4] in performing security clearances of the 3rd and 4th degrees and in acquiring information in order to ensure industrial security.

(4) The Slovak Information Service shall certify and approve the operation methods, systems and devices used in the encryption protection of information for protecting classified information of 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 realised under a specific regulation; such certification and approval of operation shall be carried out in accordance with the generally binding regulation issued by the Authority pursuant to Article 69.

Article 76
The Police Force

(1) The 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 clearance on the reliability of nominees at the place of residence of the nominee, and provide information from these clearances to the Authority,

(c) at the request of the Authority, carry out security clearance on the security of the environment in which the nominee lives, the occurrence of any potential security risks, and provide information from these clearances to the Authority,

(d) at the request of the Authority, provide information to determine the industrial security of entrepreneurs.

(2) In discharging its tasks pursuant to paragraph 1, the Police Force shall be empowered to

(a) use data from its records,,

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

(3) The Police Force in fulfilling criminal intelligence[5] tasks shall be empowered, in carrying out security clearances pursuant to Article 18(4), to use devices of operative-investigative activities and apply information-technical devices, and to keep security files on their members and on their employees.

[4] Act no. 166/2003 Coll. on the privacy protection from unauthorized use of information-technological devices and on the amendment of certain acts (Act on the Protection from Bugging)

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

PART V
CONTROL AND LIABILITY FOR A VIOLATION OF OBLIGATIONS

Article 77
Control

(1) Unless specified otherwise herein, the Authority shall, in controlling the protection of classified information in state bodies, municipalities, higher territorial units and other corporate entities, proceed as in performing a control in the state administration pursuant to a specific regulation[6].

(2) In executing control activities, members and employees of the Authority shall be empowered to

(a) be acquainted with classified information at all security classification levels to the extent necessary for the control,

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

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

(d) propose the extinction of the validity of a certificate of a person authorised to be acquainted with classified information and of a entrepreneur's industrial security certificate,

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

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

(3) The provisions of paragraph 2, except for those of points (d) to (f) shall also apply to the execution of expert activity and the preparation of expert opinions.

(4) Every person shall, in the cases specified in paragraph 2(e), be obliged to comply with a challenge of a member or employee of the Authority to surrender classified information.

Article 78
Transgressions

(1) An authorised person violating an obligation specified in Article 38 commits a transgression in the field of the protection of classified information.

(2) In addition, a person who as an unauthorised person

(a) fails to maintain confidentiality on classified information of which he/she has learnt,

(b) fails to comply with the obligation to give notice of information that has become known to him/her, or the obligation to surrender a object found containing classified information,

---

[6] National Council of the Slovak Republic Act No. 10/1996 Coll. on the control in the state administration, as amended.

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

(d) uses technical devices at variance with the provisions of this Act,

(e) Performs unauthorised aerial photographing of the territory of the Slovak Republic,

commits a transgression in the field of the protection of classified information.

(3) A fine may be imposed for a transgression

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

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

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

(4) Transgressions in the field of the protection of classified information shall be dealt with by the Authority.

(5) Transgressions and their resolution shall be governed by a specific regulation[7].

Article 79
Administrative infractions

(1) A corporate entity breaches obligations in the field of the protection of classified information, if it

(a) provides classified information to a foreign power at variance with an international agreement binding upon the Slovak Republic,

(b) fails to maintain proper records on persons authorised to be acquainted with classified information and on persons whose authorisations to do so have lapsed,

(c) fails to notify the Authority, within the period set by this Act, of the lapsing of the authorisations of persons to be acquainted with classified information of the Top Secret, Secret or Confidential security classification levels,

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

(e) fails to inform the Authority of the commencing of the realisation of tasks in the field of 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 person or with the co-participation of a foreign person,

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

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

[7] Slovak National Council Act No. 372/1990 Coll. on transgressions, as amended.

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

(j) violates any obligation imposed by this Act in the encryption protection of information,

(k) uses a technical device at variance with the provisions of this Act.

(2) For the violation of obligations specified in paragraph 1(a) to (d) a fine may be imposed of up to SKK 500 000, and for the violation of those set out in paragraph 1(e) to (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 the field of the protection of classified information.

(4) For the repeated violation of obligations in the field of the protection of classified information set out in paragraph 1 a further fine may be imposed up to double the amounts specified in paragraphs 2 and 3 within the period of two years from the date of the legal 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 under Article 79. In determining the fine, the Authority shall take in account of 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 the field of the protection of classified information 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 legal validity of the decision on its imposition.

(4) The imposition of a fine under Articles 78 and 79 shall not prejudice the provisions of specific regulations on the compensation of damages[8] nor shall obligations established by this Act lapse.

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

[8] For example, Civil Code as amended, the Labour Code as amended.

PART VI
COMMON, TRANSITIONAL AND CONCLUDING PROVISIONS

Common provisions
Article 81

(1) Generally binding legal regulations on administrative proceedings[9] shall not apply to decisions made under this Act, except for Article 55(6), Article 65(4), Articles 79 and 80.

(2) The period“state secret” or “service secret” used in laws and other generally binding legal regulations shall mean the period“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 Service, the National Bank of Slovakia, the Office of the President of the Slovak Republic, the Office of the National Council of the Slovak Republic, and the Office of the Constitutional Court of the Slovak Republic have the status of central bodies of the state administration.

Article 82

The period“Authority”, specified in Article 8(2)(f),(h),(j) to (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 Service and the Police Force of the Slovak Republic in relation to persons subjected to security clearance pursuant to Article 18(1), (2) and (4); and the period“Authority”, specified in 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 Service in relation to persons subjected 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) 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 Service and the Police Force of the Slovak Republic in connection with discharging duties in the field of criminal intelligence.

Article 84
Transitional provisions

(1) Unless specified otherwise, classified information under regulations hitherto shall remain classified information under this Act.

---

9 Act No. 71/1967 Coll.

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

(3) A person designated as at 1 November 2001 to be acquainted with service secrets shall be deemed a person authorised for the security classification level Confidential or Restricted under this Act to 31 October 2004, unless other circumstances arise causing the lapsing of the authorisation.

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

(5) An attorney, heads of other central bodies of the state administration, senior state officials and the Chairman of the Office for Protection of Personal Data shall be persons authorised to be acquainted with classified information under this Act until the elapsing of the periods of their office, but at 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 according to hitherto regulations may be used for protecting buildings and protected areas until 31 December 2005.

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

(8) Departmental encryption offices established in accordance with regulations hitherto shall be deemed departmental encryption offices established under this Act.

(9) A statement of the Authority issued according to hitherto regulations shall be deemed a certificate under this Act for the period of validity specified therein. A person so authorised to be acquainted with classified information may apply to the Authority for issuance of the certificate if he/she proves important interest in its issuance; this shall not apply to a person subjected to security clearance of any level by the Slovak Information Service, Military Intelligence Service or the Police Force pursuant to regulations hitherto.

(10) Security clearance of a nominee commenced according to hitherto regulations shall be completed in accordance with this Act.

(11) Court proceedings commenced prior to the date of this Act entering into force shall be completed according to hitherto regulations.

(12) An industrial security certificate issued according to hitherto regulations shall be deemed a certificate on industrial security issued according to this Act.

(13) Security clearance of a entrepreneur commenced according to hitherto regulations shall be completed according to hitherto regulations.

(14) A training certificate of the Authority on the protection of classified information issued according to hitherto regulations 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 regulations shall, for the period of validity stated therein, be deemed a certificate issued pursuant to this Act.

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

(17) The appointment of the Director of the Authority who has been performing the function according to hitherto regulations shall be deemed an appointment pursuant to this Act.

Article 84(a)

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

Article 85
Repealing provisions

The following shall be repealed:

1. Article I of Act no. 241/2001 Coll. on the protection of classified information and amending certain 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,
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 III

National Council of the Slovak Republic Act No. 162/1993 Coll. on identification cards, as amended by National Council of the Slovak Republic Act No. 13/1996 Coll., National Council of the Slovak Republic Act No. 222/1996 Coll., Act No. 441/2001 Coll. and Act No. 660/2002 Coll. shall be supplemented as follows:

In Article 15a(3), a comma and the words “National Security Authority” shall be inserted after the words “the Military Intelligence Service”.

Article IV

National Council of the Slovak Republic Act No. 272/1994 Coll. on the protection of human health, as amended by National Council of the Slovak Republic Act No. 222/1996 Coll., National Council of the Slovak Republic Act No. 290/1996 Coll., Act No. 95/2000 Coll., Act No. 470/2000 Coll., Act No. 514/2001 Coll., Act No. 553/2001 Coll., Act No. 245/2003 Coll., Act No. 256/2003 Coll., Act No. 427/2003 Coll., and Act No. 578/2003 Coll. shall be amended as follows:

In Article 38(1) the following point (f) shall be inserted:

“(f) of the National Security Authority the Ministry of Interior of the Slovak Republic, in cooperation with the National Security Authority.”.

Article V

National Council of the Slovak Republic Act No. 277/1994 Coll. on health care, as amended by National Council of the Slovak Republic Act No. 98/1995 Coll., National Council of the Slovak Republic Act No. 110/1996 Coll., National Council of the Slovak Republic Act No. 222/1996 Coll., Act No. 140/1998 Coll., Act No. 241/1998 Coll., Act No. 80/2000 Coll., Act No. 416/2001 Coll., Act No. 553/2001 Coll., Act No. 118/2002 Coll., Act No. 131/2002 Coll., Act No. 219/2002 Coll., Act No. 450/2002 Coll., Act No. 457/2002 Coll., Act No. 138/2003 Coll., Act No. 445/2003 Coll., Act No. 528/2003 Coll., and Act No. 578/2003 Coll. shall be amended as follows:

1. In Article 80(1)(e) shall be worded as follows:

"(e) of the Slovak Information Service and of the National Security Authority the Ministry of Interior of the Slovak Republic, in agreement with the Slovak Information Service and with the National Security Authority.".

2. Article 80(2) shall be worded as follows:

"(2) The organisation and the provision of healthcare in the armed forces, the Police Force, the Prison and Judiciary Guard Corps, the National Security Authority and the Slovak Information Service shall be provided for by generally binding legal regulations, issued by the individual central bodies of the state administration, laying down and implementing the state administration in the field of healthcare pursuant to paragraph 1, in agreement with the Ministry of Health.".

Article VI

National Council of the Slovak Republic Act No. 330/1996 Coll. on safety and protection of health at work, as amended by Act No. 95/2000 Coll. and Act No. 158/2001 Coll. shall be supplemented as follows:

In Article 7a(2) a comma and the words "the National Security Authority" shall be inserted after the words "the Slovak Information Service".

Article VII

Act No. 280/1997 Coll. on the Common Health Insurance Company, as amended by Act No. 242/2000 Coll., Act No. 362/2000 Coll., Act No. 291/2002 Coll., Act No. 457/2002 Coll., and Act No. 442/2003 Coll. shall be supplemented as follows:

In Article 10(1) the following point (i) shall be inserted:

"(i) members of the National Security Authority" (hereinafter referred to as "the Security Authority").".

Article VIII

Act No. 381/1997 Coll. on travel documents, as amended by Act No. 441/2001 Coll., Act No. 48/2002 Coll., and Act No. 660/2002 Coll. shall be amended as follows:

In Article 7(1), a new point (j) shall be inserted after the point (i), worded as follows:
"(j) the Director of the National Security Authority,".

The points (j), (k), (l), (m) and (n) shall be designated as points (k), (l), (m), (n) and (o).

Article IX

Act No. 70/1998 Coll. on the power industry and on the amendment of Act No. 455/1991 Coll. on trades (Trading Act), as amended, amended by Act No. 276/2001 Coll., Act No. 208/2002 Coll., Act No. 405/2002 Coll., and Act No. 24/2004 Coll. shall be supplemented as follows:

1. In Article 9(6)(d), a comma and the words "the National Security Authority" shall be inserted after the words "the Slovak Information Service".

2. In Article 9(14) a comma and the words "the National Security Authority" shall be inserted after the words "the Slovak Information Service".

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 supplementing of certain acts".

Article XI

Act No. 95/2000 Coll. on labour inspection and on the amendment and supplementing of certain acts, as amended by Act No. 311/2001 Coll. and Act No. 231/2002 Coll. shall be supplemented as follows:

In Article 2(5(b), the words "and workplaces of the National Security Authority," shall be inserted after the words "the Slovak Information Service".

Article XII

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

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

Slovak National Council Act No. 511/1992 Coll. on the administration of taxes and fees and on adjustments in the system of territorial financial authorities, as amended by National Council of the Slovak Republic Act No. 102/1993 Coll., National Council of the

Slovak Republic Act No. 165/1993 Coll., National Council of the Slovak Republic Act No. 253/1993 Coll., National Council of the Slovak Republic Act No. 254/1993 Coll., National Council of the Slovak Republic Act No. 172/1994 Coll., National Council of the Slovak Republic Act No. 187/1994 Coll., National Council of the Slovak Republic Act No. 249/1994 Coll., National Council of the Slovak Republic Act No. 367/1994 Coll., National Council of the Slovak Republic Act No. 374/1994 Coll., National Council of the Slovak Republic Act No. 58/1995 Coll., National Council of the Slovak Republic Act No. 164/1995 Coll., National Council of the Slovak Republic Act No. 304/1995 Coll., National Council of the Slovak Republic Act No. 386/1996 Coll., Act No. 12/1998 Coll., Act No. 219/1999 Coll., Act No. 367/1999 Coll., Act No. 240/2000 Coll., Act No. 493/2001 Coll., Act No. 215/2002 Coll., Act No. 233/2002 Coll., Act No. 291/2002 Coll., Act No. 526/2002 Coll., Act No. 114/2003 Coll., and Act No. 609/2003 Coll. shall be supplemented as follows:

In Article 23(5), the following point (zb) shall be inserted:
"(zb) to the National Security Authority for the purposes of discharging security clearances under a specific regulation[8l)].

The footnote 8l shall have the following text:
"8l) Act No. .../2004 Coll. on the protection of classified information and on the supplementing of certain acts.

Article XVII

Act No. 483/2001 Coll. on banks and on the amendment of certain 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 the protection of classified information and on the amendment of certain acts.".

Article XVIII

Abolished from 01.12.2011

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 certain 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 certain acts” shall be added.

Article XX

Act No. 575/2001 Coll. on the organisation of activities of the Government and organisations 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 certain acts.”.

Article XXI

Force of legislation

This Act shall enter into force on 1 January 2004.

Finding no. 638/2005 Coll entered into force on 30 December 2005.

Law no. 255/2006 Coll entered into force on 11 May 2006.

Law no. 330/2007 Coll entered into force on 1 January 2008.

Law no. 668/2007 Coll entered into force on 1 February 2008.

Finding no. 290/2009 Coll and Act. 291/2009 Coll entered into force on 17 July 2009.

Law no. 400/2009 Coll entered into force on 1 November 2009.

Law no. 192/2011 Coll entered into force on 1 August 2011.

Law no. 392/2011 Coll entered into force on 1 December 2011.

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. …/2004 Coll.

State Security Structures Pursuant to Article 14(1)

Under this Act a member 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 (ČSSR) for the management of the Federal Intelligence Service (1970-1971),
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) (1969-1971),
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. ŠtB Regional directorates (1953-1963) and their subordinated units,
14. MoI Directorate II (1953-1963),
15. MoI Directorate II (later of Federal MoI, 1964-1974),
16. MoI Directorate III (1953-1963),
17. MoI Directorate IV (1953-1963),
18. MoI Directorate V (1952-1962),
19. MoI Directorate VI (1953-1963),
20. Federal MoI Directorate XI (later ZNB),
21. 1st, 2nd, 3rd, 4th, 5th independent sector of the Ministry of National Security (1950-1951),
22. Divisions O, Z, C, E, T, V, LM of the Ministry of National Security (1951-1952),
23. Operative divisions and departments of the Presidential Protection Directorate (1952-1953), 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, empowered to execute 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. …/2004 Coll.

Data Required in the Personal Questionnaire of a Person

1. Name, surname, academic titles.
2. Date and place of birth, birth registration number.
3. Address of permanent and temporary residence.
4. Marital status.
5. Nationality, or any other nationality, changes to nationality.
6. Citizenship pass number, travel document number and place of issue.
7. If concerning a foreign person, stays in the Slovak Republic longer than 30 days over the last seven years.
8. Education, summary of schools attended.
9. Employment, registered office of the employer, position, function held.
10. Summary of previous employers.
11. Conduct of business activities.
12. Personal data of spouse, common-law spouse, children – first names, surnames, including maiden names, date and place of birth, permanent address, temporary address, nationality, employment.
13. All criminal charges brought against the person.
14. Sanctions for transgressions, other administrative infractions over the last five years.
15. Current or past addiction to alcoholic beverages.
16. Cooperation with State Security in the categories resident, agent, secret collaborator, holder of a leased flat and informer.
17. Opinion on the security risks pursuant to Article 14(2).

Annex No. 3 to Act No. …/2004 Coll.

Data Required in the Personal Security Questionnaire

A. General Part

1. Name, surname, academic titles.
2. Date and place of birth, birth registration number.
3. Address of permanent and temporary residence.
4. Marital status.
5. Nationality, or any other nationality, changes to nationality.
6. Citizenship pass number, travel document number and place of issue.
7. If concerning a foreign person, stays in the Slovak Republic longer than 30 days over the last seven years.
8. Education, summary of schools attended.
9. Language skills.
10. Employment, registered office of the employer, position, function held.
11. Summary of previous employers, including positions.
12. Conduct of business activities.
13. Where this concerns a soldier, the place and duration of the basic military service, other services in the armed forces, rank attained.
14. Where this concerns a member of the Police Force, the place and duration of service, rank attained.
15. Personal data of spouse, common-law spouse, children, parents, siblings - first names, surnames, including maiden names, date and place of birth, birth registration number, permanent address, temporary address, nationality, employment.
16. All criminal charges brought against the person.
17. Sanctions for transgressions, other administrative infractions over the last five years.
18. Current or past addiction to alcoholic beverages.
19. Current or past use of narcotics or psychotropic substances.
20. Property relations, all financial liabilities with a total sum exceeding SKK 100 000.
21. Decisions on execution orders over the last seven years.
22. Scope of acquaintance with classified information hitherto.
23. Cooperation with a former or current intelligence service of a foreign power, study stays and courses attended in that service, knowledge ofthat service’s interest in the nominee.
24. Cooperation with State Security in the categories resident, agent, secret collaborator, holder of a leased flat and confidential person.
25. Opinion on the security risks pursuant to Article 14(2).
26. Solemn declaration on the veracity of the data stated.

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, of the common-law spouse – first names, surnames, including maiden names, date and place of birth, birth registration number, permanent address, nationality, employment.
2. Membership of, and relationship to civic associations, political movements and parties, churches, religious societies, domestic and foreign organisations.

3. First name, surname and address of two persons familiar with the nominee able to provide information on the data in the security questionnaire (family members or persons with confidential relations, e.g. managing property affairs, are not eligible).
4. Stays abroad longer than 30 days after reaching 18 years of age -– for the private, business, or gainful purposes.
5. Any psychiatric examination and treatment undergone.

Annex No. 4 to Act No. …/2004 Coll.

Data Required in the Security Questionnaire of a entrepreneur

The Security Questionnaire of a entrepreneur shall contain the following:

(a) identification data of the entrepreneur, in particular name, registered office, identification number, year of establishment, previous registered offices, legal form of business, business licence, extract from the Commercial Register, tax identification number, number of employees,
(b) economic data on the entrepreneur, in particular financial results for the last five years, auditors' reports, subject of business,
(c) property data of the entrepreneur, in particular commercial assets, liabilities, data on net equity,
(d) business relations to the entrepreneur, in particular an overview of foreign partners,
(e) an overview of financial institutions in which the entrepreneur has opened or maintains an account over the last three years,
(f) an overeview of loans and credit provided as well as repaid over the last five years,
(g) data on any petitions for bankruptcy, settlement, data on the entrepreneur's entry into liquidation,
(h) name and registered office of the tax advisor,
(i) financial liabilities toward state bodies, entrepreneurs, insurance companies, other corporate entities and individuals,
(j) a list of the entrepreneur's employees who are not citizens of the Slovak Republic,
(k) a list of the entrepreneur's managerial staff for the last three years,
(l) data on members of the statutory body, in particular personal data of the statutory body (first name, surname, birth registration number, permanent address, temporary address, nationality), appointment of other corporate entities in which the members of the statutory body have been or are partners, executives or members of the supervisory board, a list of managerial staff with whom the employment relationship has been periodinated over the last three years.