

Classified Information Protection Act

Promulgated, SG No. 45/30.04.2002, corrected, SG No. 5/17.01.2003, amended, SG No. 31/4.04.2003, supplemented, SG No. 52/18.06.2004, SG No. 55/25.06.2004, SG No. 89/12.10.2004, amended, SG No. 17/24.02.2006, effective 1.05.2006, amended, SG No. 82/10.10.2006, SG No. 46/12.06.2007, effective 1.01.2008, SG No. 57/13.07.2007, effective 13.07.2007, amended and supplemented, SG No. 95/20.11.2007, SG No. 109/20.12.2007, effective 1.01.2008, SG No. 36/4.04.2008, supplemented, SG No. 66/25.07.2008, effective 26.09.2008, amended, SG No. 69/5.08.2008, supplemented, SG No. 109/23.12.2008, amended and supplemented, SG No. 35/12.05.2009, effective 12.05.2009, supplemented, SG No. 42/5.06.2009, amended, SG No. 82/16.10.2009, amended and supplemented, SG No. 93/24.11.2009, effective 25.12.2009, amended, SG No. 16/26.02.2010, effective 26.02.2010, SG No. 88/9.11.2010, effective 1.01.2011, SG No. 23/22.03.2011, effective 22.03.2011, SG No. 48/24.06.2011, effective 24.06.2011, supplemented, SG No. 80/14.10.2011, effective 14.10.2011, amended and supplemented, SG No. 44/12.06.2012, effective 1.07.2012, supplemented, SG No. 103/28.12.2012, amended and supplemented, SG No. 52/14.06.2013, effective 14.06.2013, amended, SG No. 70/9.08.2013, effective 9.08.2013, SG No. 49/13.06.2014, amended and supplemented, SG No. 53/27.06.2014, SG No. 14/20.02.2015, amended, SG No. 61/11.08.2015, effective 1.11.2015, amended and supplemented, SG No. 79/13.10.2015, effective 1.11.2015, SG No. 28/8.04.2016; Decision No. 7 of the Constitutional Court of the Republic of Bulgaria of 21.06.2016 - SG No. 49/28.06.2016; supplemented, SG No. 62/9.08.2016, effective 9.08.2016, amended and supplemented, SG No. 71/13.09.2016, SG No. 81/14.10.2016, effective 1.01.2017, supplemented, SG No. 97/5.12.2017, SG No. 103/28.12.2017, effective 1.01.2018, amended, SG No. 7/19.01.2018, supplemented, SG No. 17/23.02.2018, effective 23.02.2018, amended and supplemented, SG No. 44/29.05.2018, amended, SG No. 77/18.09.2018, effective 1.01.2019, amended and supplemented, SG No. 88/23.10.2018, amended, SG No. 17/26.02.2019, amended and supplemented, SG No. 60/7.07.2020, effective 1.10.2020, amended, SG No. 69/4.08.2020, supplemented, SG No. 105/11.12.2020, effective 1.01.2021, amended, SG No. 80/24.09.2021, supplemented, SG No. 62/5.08.2022, amended and supplemented, SG No. 84/6.10.2023, effective 6.10.2023

Chapter One GENERAL PROVISIONS

Article 1

(1) This Act governs the public relations arising in connection with the generation, the processing, and the storing of classified information, and lays down the conditions and procedure for the release thereof and the access thereto.

(2) The purpose of this Act is to protect classified information from unauthorised access.

(3) Within the meaning of this Act, "classified information" is any information which is a State secret or an official secret, and any foreign classified information.

Article 2

This Act shall apply as well to any foreign classified information which may be made available by another State or an international organisation, insofar as an existing international treaty, to which the Republic of Bulgaria is a party, does not provide otherwise.

Article 3

(1) Access to classified information shall not be allowed to any person other than those having an appropriate clearance in keeping with the "need- to-know" principle, unless otherwise provided hereunder.

(2) The "need-to-know" principle is the restriction of access to particular classified information to such persons whose official duties, or a special assignment, require such access.

Chapter Two

CLASSIFIED INFORMATION PROTECTION AUTHORITIES

Section I

State Information Security Commission

Article 4

(1) The State Information Security Commission (SISC) is a government authority which shall conduct the classified information protection policy of the Republic of Bulgaria.

(2) The State Information Security Commission is a first-tier obligor of budget funds.

Article 5

The State Information Security Commission shall be supported by an administration of which the activities, structure and operation shall be laid down in Institutional Rules adopted by the Council of Ministers.

Article 6

(1) The State Information Security Commission is a collegiate body comprised of five members, including a chairperson and a vice chairperson, who shall be appointed by the Council of Ministers for a term of five years, subject to the advice of the Prime Minister.

(2) No person may be a member of the Commission unless such person is a university graduate.

Article 6a

(New, SG No. 95/2007)

(1) The chairperson of the Commission shall receive basic monthly salary amounting to 90 percent of the basic monthly salary of the Speaker of the National Assembly.

(2) The vice chairman of the Commission shall receive basic monthly salary amounting to 90 percent, and the members - 85 percent of the salary of the chairperson of the Commission.

(3) The basic monthly salary shall be reviewed quarterly in view of the average monthly salary for the last month of the preceding quarter.

Article 7

(1) The SISC chairperson shall submit an annual report to the Council of Ministers on the overall activity relating to the protection of classified information.

(2) The Council of Ministers shall introduce the report under paragraph 1 before the National Assembly, which shall adopt it by its decision.

(3) The SISC chairperson shall provide the same volume and content of information on the Commission's activities to the Speaker of the National Assembly, to the President of the Republic, and to the Prime Minister.

Article 8

The State Information Security Commission shall have a duty to:

1. organise, perform, coordinate and control the activities relating to the protection of classified information;

2. provide equal protection of classified information;

3. perform its activities in close collaboration with the authorities of the Ministry of Defence, of the Ministry of Home Affairs, of the Ministry of Foreign Affairs, and with the security services and the public order services.

Article 9

For the purposes of performing its activities, SISC shall have a duty to:

1. develop guidelines and approve plans of action for organisational units in the event of a threat to the interests of the State resulting from unauthorised access to classified information;

2. analyse and assess the state of preparedness for the protection of classified information in the event of a threat to any interest protected by law resulting from unauthorised access to classified information, and shall issue mandatory instructions in that area;

3. organise and perform activities to prevent and mitigate the harmful consequences of unauthorised access to classified information;

4. draft and introduce before the Council of Ministers for adoption statutory instruments relating to the protection of classified information;

5. organise and ensure the functioning of registries in the field of international relations;

6. organise, control, and be responsible for, the performance of obligations relating to the protection of classified information as laid down in international treaties to which the Republic of Bulgaria is a party;

7. provide general direction of the activities relating to the background investigation of the persons who require to operate with classified information, and relating to the issuance of the appropriate levels of clearance for access to classified information ("clearance");

8. provide general direction of the activities relating to the background investigation of natural or legal persons proposing to enter or performing a contract which involves access to classified information, and shall approve a sample security certificate under this Act ("certificate");

9. jointly with the security services, conduct background investigations of, and subject to the advice of such services, issue clearance to, persons nominated for appointment as information security officers;

9a. (new, SG No. 71/2016) conduct background investigation jointly with the security services and the public order services in the cases under Article 45a, paragraph 3 and issue or deny clearance for access to classified information;

10. issue documents certifying to such foreign authorities as it may concern that Bulgarian natural or legal persons have been issued with clearance or certificate, as the case may be;

11. jointly with the security services, conduct background investigations of Bulgarian citizens who apply for a position or for the performance of a special assignment which requires such citizens to operate with the classified information of another State or of an international organisation, at the written request of the competent information security authority of such State or international organisation;

12. maintain single registers of clearances, certificates, certifying or confirming documents issued, revoked or terminated, and of refusals to issue or terminate such papers, and a register of the materials and documents which contain classified information, such information being a State secret or an official secret;

13. advise immediately the Prime Minister in the event of unauthorised access to information classified as "Top Secret";

14. organise and coordinate the training for operation with classified information;

15. provide technical guidance to information security officers;

16. (amended, SG No. 88/2018) exercise general control over the protection of such classified information as is generated, stored, processed or transmitted in communication and information systems;

17. issue visit permits to persons performing inspections in pursuance of international treaties relating to the reciprocal protection of classified information;

18. (new, SG No. 81/2016, effective 1.01.2017) receive, store, transport and deliver documents and/or materials, containing classified information;

19. (new, SG No. 97/2017) receive, store, transport and deliver documents and/or materials of the MoI, containing unclassified information, that can not be transported in accordance with the procedure established by the Postal Services Act.

Article 10

(1) For the purposes of performing its functions and activities under Article 9, SISC:

1. may require information from the information bases of the security services and the public order services;

2. shall be provided, immediately upon request and free of charge, with the necessary information by the government authorities and by the authorities of local self-government;

3. shall be provided, immediately upon request and free of charge, with the necessary information by any natural or legal person in accordance with the existing legislation. Such persons may refuse to provide such information as is unrelated to a background investigation to which they had consented or of which they had been properly notified;

4. shall issue mandatory instructions to the persons responsible hereunder.

(2) The conditions and procedure for the provision of information under subparagraphs 1 2 and 3 of paragraph 1 shall be laid down in the Detailed Rules for the Application hereof.

(3) (New, SG No. 81/2016, effective 1.01.2017) For the purpose of performing their official duties the authorities that receive, transport and deliver documents and/or materials, containing classified information, shall have the right to use force and technical aids in the event of attempts at unauthorised access to the documents and/or materials only when that is absolutely necessary.

(4) (New, SG No. 81/2016, effective 1.01.2017) The organisation of the activities that involve reception, sorting, describing, storing, transportation and delivery of documents and/or materials, containing classified information, shall be set out in rules approved by the chairperson

of SCIS.

Article 10a. (New, SG No. 81/2016, effective 1.01.2017) (1) The provisions regarding civil service in the Ministry of Interior Act shall apply to the SCIS officers, whose official duties involve performing the function under Article 9, paragraph 18.

(2) The chairperson of SCIS shall be the appointing authority under paragraph 1.

Article 10b. (New, SG No. 81/2016, effective 1.01.2017) (1) The SCIS chairperson shall approve a classification of positions in SCIS for the officers referred to in Article 10a and shall issue an order for its implementation.

(2) The procedure for the development and approval of job descriptions, their types and content shall be determined by an order of the SCIS chairperson.

Article 10c. (New, SG No. 81/2016, effective 1.01.2017) Civil servants under the Civil Servants Act may be reappointed as civil servants for positions under Article 10a, paragraph 1 without a competitive examination procedure if they meet the requirements for appointment to the respective position.

Article 10d. (New, SG No. 81/2016, effective 1.01.2017) A competitive examination procedure for the appointment of civil servants under Article 10a, paragraph 1 in SCIS shall not be held for persons, who are civil servants in the security services or the public order services or in other departments and institutions to which the provisions of the Ministry of Interior Act regarding civil service apply, if they meet the requirements for appointment to the respective position.

Section II

Functions of the Security Services

Article 11

(1) The security services shall have a duty to:

1. conduct background investigations of their officers and applicants for appointment, and shall issue, revoke or terminate the clearances of such officers or applicants;

2. conduct background investigations of natural or legal persons proposing to enter or performing a contract which involves access the classified information, and shall issue certificates of compliance with the security requirements hereunder;

3. provide assistance to SISC with the performance of its functions under Article 9, paragraphs 9, 10, 11, 13, 14 and 17;

4. provide assistance with the performance of the functions under paragraph 2, subparagraph 3 of this Article and under Article 12(2).

(2) (Amended, SG No. 109/2007) The State Agency for National Security shall, in addition to its duties under paragraph 1, have a duty to:

1. conduct background investigations of the persons who require to operate with classified information, and shall issue, revoke, terminate or deny clearance for access, except in the circumstances under Article 22, paragraph 1, subparagraph 5;

2. issue confirming documents to foreign natural or legal persons on the basis of clearance or certificate issued by the appropriate competent authority of another State or of an international organisation and subject to a background investigation conducted in the Republic of Bulgaria ("confirmation"), except in the circumstances under paragraph 3, subparagraph 3;

3. exercise direct control over the protection of classified information and the compliance with the relevant legal provisions.

(3) (Amended, SG No. 109/2007, SG No. 35/2009, effective 12.05.2009, SG No. 69/2020) Within the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army, excepting the Military Intelligence Service, State Agency for National Security shall, in addition to its duties under paragraph 1 and paragraph 2, Item 3, have a duty to:

1. (amended, SG No. 46/2007, SG No. 35/2009, effective 12.05.2009) conduct background investigations and issue, revoke, and terminate the clearances of Bulgarian citizens, enlisted or servicemen, reservists or civilian employees officially appointed to, or employed by, the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army;

2. (amended, SG No. 35/2009, effective 12.05.2009) conduct background investigations and issue, revoke, and terminate the clearances of natural persons or the certificates of legal persons proposing to perform or performing an activity for the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army;

3. (amended, SG No. 35/2009, effective 12.05.2009) issue confirmations to foreign citizens for the purposes of work and/or training at the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army;

(4) In pursuance of their duties under paragraphs 1, 2 and 3, the security services shall have a right to:

1. apply and make use of intelligence gathering techniques under such conditions and procedure as shall be laid down in law;

2. apply and make use of special surveillance devices under the conditions and procedure laid down in the Special Intelligence Means Act with respect to any applicant for access to information classified as "Top Secret";

3. make use of data available in their information bases relating to any natural or legal person who is the subject of a background investigation;

4. store the data gathered in the course of the background investigation of any natural person or any bidder, whether a natural or a legal person, for the purposes of entering or performing a contract which involves access to classified information;

5. store data relating to cases of unauthorised access to classified information;

6. the necessary information to be provided by any government authority or local self-government authority, or natural or legal person in accordance with the existing legislation. The conditions and procedure for the provision of such information shall be laid down in the Detailed Rules for the Application hereof.

(5) In pursuance of their duties under paragraphs 1-4, the security services shall collaborate with one another.

Article 12

(Amended, SG No. 109/2007)

For the purposes of exercising direct control over the protection of classified information and the compliance with the relevant legal provisions, the Chairperson of the State Agency for National Security shall issue an order in writing to designate officers who shall have a right to:

1. access to the sites and premises of the controlled organisational units, including the right to perform physical inspections of such sites and premises;

2. access to the documents relating to the arrangements made for the protection of classified information at the controlled organisational units;

3. (amended, SG No. 88/2018) access communication and information systems, including information systems connected thereto, for the purpose of ascertaining the reliability of

protection;

4. where necessary, require written or oral explanations from the heads or the officers of the controlled organisational units;

5. for the purposes of an inspection at a controlled organisational unit, require information from other organisational units and, where necessary, explanations from the heads or officers thereof, relating to the generation, the processing, the storing or the release of classified information;

6. use experts where special expertise is necessary to establish facts and circumstances in the course of an inspection;

7. prescribe concrete measures relating to the protection of classified information.

Article 13

The procedure for the inspections under Article 12 shall be laid down in a Regulation by the Council of Ministers.

Article 14

(Amended, SG No. 109/2007)

The State Agency for National Security shall have a duty to:

1. (amended, SG No. 17/2006, SG No. 109/2007) perform the activities relating to the cryptographic protection of classified information in pursuance of the State Agency for National Security Act.

2. (supplemented, SG No. 103/2012, amended, SG No. 88/2018) issue, revoke and terminate security certificates for communication and information systems;

3. (amended, SG No. 88/2018) coordinate and control TEMPEST countermeasures;

4. provide and control the training of persons cleared for access to classified information in the use of cryptographic methods and devices.

Section III

Public Order Services

Article 15

The public order services shall conduct background investigations of their officers and applicants for appointment, and shall issue, revoke or terminate the clearances thereof.

Article 16

(1) In pursuance of their duties under Article 15, the public order services shall have a right to:

1. apply and make use of operational search techniques and devices under such conditions and procedure as shall be laid down in law;

2. make use of data available in their information bases relating to any natural or legal person who is the subject of a background investigation;

3. store the data gathered in the course of the background investigation of their officers;

4. store data relating to cases of unauthorised access to classified information by the officers under Article 15;

5. the necessary information to be provided by other organisational units in connection with

a background investigation under Article 15.

(2) The public order services shall, within the limits of their duties and powers, provide assistance to the security services in connection with the pursuance of their duties under Article 11.

Section IV

Duties of Organisational Units

Article 17

The organisational units shall have a duty to:

1. apply the requirements relating to the protection of classified information and control compliance therewith;
2. be responsible for the protection of information;
3. in the event of unauthorised access to classified information, advise immediately SISC and take action to limit the harmful consequences;
4. provide the information under Article 10(1), subparagraph 2, Article 11(4), subparagraph 6, and Article 16(1), subparagraph 5.

Article 18

(1) The officers of organisational units cleared for access to a particular level of classified information shall have a duty to:

1. protect such classified information from unauthorised access;
2. advise immediately the information security officer in the event of unauthorised access to classified information;
3. advise the information security officer of all modifications to classified materials and documents where unauthorised access is not the case;
4. undergo medical examinations from time to time, but not less frequently than once in every two years, and psychological tests under the conditions and procedure laid down in Article 42(3).

(2) Every person cleared for access to information classified as "Top Secret" shall have a duty to notify the information security officer of every intended private foreign travel prior to the date of departure, except where such travel is to any State with which the Republic of Bulgaria has concluded a treaty on the reciprocal protection of classified information.

(3) The provisions of paragraph 2 shall not apply to the persons under Article 39(1).

(4) The officers of the security services and the public order services shall notify in writing their superiors of every intended foreign travel.

(5) (Amended, SG No. 109/2007, SG No. 36/2008, SG No. 35/2009, effective 12.05.2009, repealed, SG No. 16/2010, effective 26.02.2010).

Article 19

Every person cleared for access to classified information in connection with a special assignment shall have a duty to comply with the conditions and procedure for the protection of classified information.

Section V

Information Security Officer

Article 20

(1) The head of each organisational unit shall direct, organise and control the activities relating to the protection of classified information.

(2) The head of each organisational unit shall appoint an information security officer subject to that person being cleared by SISC for access to classified information.

(3) By way of an exception, depending on the level and volume of classified information, the head of an organisational unit may perform the functions of information security officer, provided that he shall meet the requirements under Article 21.

(4) The information security officer shall report directly to the head of the organisational unit.

Article 21

(1) No person may be appointed information security officer unless he meets the following requirements:

1. such person is a Bulgarian citizen and not simultaneously the citizen of any other State; and

2. has been cleared for access to the appropriate level of classified information under the conditions and procedure laid down in Chapter Five.

(2) Upon his appointment, the information security officer shall undergo training in the protection of classified information.

Article 22

(1) The information security officer shall have a duty to:

1. ensure compliance with the provisions of this Act and of the international treaties relating to the protection of classified information;

2. apply the rules relating to the types of classified information protection;

3. develop a security plan for the organisational unit, providing for physical and technical security measures, and ensure its implementation;

4. inspect from time to time the records and the flow of materials and documents;

5. conduct ordinary background investigation under Article 47;

6. administer the procedure for ordinary background investigation within the organisational unit and maintain a register of persons so investigated;

7. advise SISC accordingly upon the expiration of clearances, the termination or relocation of officers, or, as the case may be, of the need to modify a clearance for access to a particular level of classified information;

8. advise, immediately and in writing, SISC and the appropriate service of any change of circumstances relating to clearances, certificates, certifying documents or confirmations issued;

9. maintain a record of the cases of unauthorised access to classified information and of actions taken, and advise SISC immediately of each such case and action;

10. ensure the classification of information at the appropriate level;

11. develop a plan for the protection of classified information during a state of war, martial law or any other state of emergency;

12. organise and administer the training of the organisational unit officers in the protection of classified information.

(2) Upon the occurrence of circumstances under paragraph 1, subparagraph 7, 8 or 9, the

information security officers of the security or the public order services shall immediately advise the respective head of service.

(3) (Amended, SG No. 109/2007, SG No. 35/2009, effective 12.05.2009) The information security officers of the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army shall, upon the occurrence of circumstances under paragraph 1, subparagraph 8 or 9, immediately advise the State Agency for National Security.

Section VI

Administrative Units for Information Security

Article 23

In pursuance of his duties under Article 22, and depending on the volume of classified information, the information security officer may be supported by an administrative unit for information security.

Article 24

No person may be appointed to any unit under Article 23 unless he meets the requirements under Article 21.

Chapter Three

CLASSES OF CLASSIFIED INFORMATION AND CLASSIFICATION LEVELS

Section I

Classified Information

Article 25

State secret is such information, as listed in Schedule 1, the unauthorised access to which might threaten or prejudice such interests of the Republic of Bulgaria as relate to national security, defence, foreign policy or the protection of the constitutional order.

Article 26

(1) Official secret is such information as is generated or stored by government authorities or by the authorities of local self government, is not a State secret, and the unauthorised access to which might adversely affect the interests of the State or prejudice another interest protected by law.

(2) The information which shall be the subject of classification as an official secret shall be determined by law.

(3) The heads of organisational units shall, within the limits hereunder, announce a list of the classes of information under paragraph 2 within their respective field of activity. The procedure for, and the manner of, such announcement shall be laid down in the Detailed Rules for the Application hereof.

Article 27

Foreign classified information is such classified information as has been disclosed by another State or by an international organisation in pursuance of an international treaty to which the Republic of Bulgaria is a party.

Section II

Classification Levels

Article 28

(1) The information classification levels and their respective wordings shall be the following:

1. "Top Secret";
2. "Secret";
3. "Confidential";
4. "Four Official Use Only".

(2) The information which is a State secret shall be marked for security level as follows:

1. where the unauthorised access to such information might pose an exceptionally high threat to the sovereignty, the independence or the territorial integrity of the Republic of Bulgaria, or to its foreign policy or international relations in the field of national security, or might pose a threat of irreparable or exceptionally grave damage, or cause such damage in the field of national security, defence, foreign policy or the protection of the constitutional order, - "Top Secret";

2. where unauthorised access to such information might pose a high threat to the sovereignty, the independence or the territorial integrity of the Republic of Bulgaria, or to its foreign policy or international relations in the field of national security, or might pose a threat of nearly irreparable or grave damage, or cause such damage in the field of national security, defence, foreign policy or the protection of the constitutional order, - "Secret";

3. where unauthorised access to such information might pose a threat to the sovereignty, the independence or the territorial integrity of the Republic of Bulgaria, or to its foreign policy or international relations in the field of national security, or might pose a threat of damage, or cause damage in the field of national security, defence, foreign policy or the protection of the constitutional order, - "Confidential".

(3) The information classified as an official secret shall be marked "Four Official Use Only".

(4) With a view to ensuring a higher level of protection, as necessary having regard to the character of the subject information or the provisions of international treaties to which the Republic of Bulgaria is a party, SISC may by its decision, subject to the advice of the Minister of Home Affairs or the Minister of Defence or any of the directors of the security services, prescribe:

1. additional markings for materials and documents classified higher than "Top Secret";
2. a special procedure for the generation, use, reproduction, release, and storage of such materials and documents;
3. the categories of persons cleared for access to such materials and documents.

Article 29

The classification levels of foreign classified information received by the Republic of Bulgaria from, or of classified information disclosed by the Republic of Bulgaria to, another State

or an international organisation, in pursuance of an international treaty which has come into force for the Republic of Bulgaria and for that other State or international organisation, shall be aligned in accordance with such treaty.

Chapter Four

MARKING OF INFORMATION

Section I

Marking Procedure of Classified Information

Article 30

- (1) Classified information shall be identified by an appropriate security marking.
- (2) Such security marking shall contain:
 1. Classification level.
 2. Date of classification.
 3. Date on which the classification period shall expire, where such date is different from the date on which the appropriate period under Article 34(1) shall expire.
 4. Legal reasons for classification.
- (3) A compilation of materials and/or documents which are individually identified by different security markings shall be identified in its entirety by the appropriate security marking of that material or document contained in the compilation which is classified at the highest level.

Article 31

- (1) The appropriate security marking shall be determined by the authorised signer of the document which contains classified information or certifies the existence of classified information in a material other than that document.
- (2) The person who has generated a document or material containing classified information, where such person is other than the person under paragraph 1, shall identify such document by an appropriate security marking which shall be valid until the final determination of the security marking by the person under paragraph 1.
- (3) The persons who have a duty to mark classified information shall be responsible for marking or the omission to mark such information.
- (4) The making, the modification or the deletion of a security marking shall not be allowed outside the clearance limits of the person who makes or modifies or deletes such marking.
- (5) Classified information may not be identified by any security marking other than the one appropriate to the classification level as determined in pursuance of this Act and the Detailed Rules for the Application hereof.
- (6) The level at which information is classified may not be modified or removed without the consent of the person under paragraph 1 or of such person's superior.
- (7) The level at which information is classified may not be modified without a valid reason.
- (8) Whoever, having lawfully received classified information, finds that such information has been classified at other than the appropriate level shall immediately advise the person under paragraph 1 or such person's superior.
- (9) If the person so advised chooses to modify the level at which the information is classified, he shall immediately advise the recipient thereof. Upon submission of classified

information to third parties the recipient shall immediately advise those parties on the modification.

(10) The heads of organisational units shall organise the training of their officers in the conditions and procedure for the security marking of information (the making, modification, and deletion of security markings) under the technical guidance of SISC.

Article 32

The procedure for, and the manner of, the security marking of information shall be laid down in the Detailed Rules for the Application hereof.

Section II

Storing of Classified Information

Article 33

(1) Classified information shall be generated, processed, released, stored, and destroyed under the conditions and procedure laid down in this Act and in the implementing statutory instruments hereto, and in accordance with the types of protection provided for, and corresponding to, the classification level, except as otherwise may be provided in an international treaty to which the Republic of Bulgaria is a party.

(2) (Amended, SG No. 57/2007) Within one year from the expiration of the protection period, the information shall be transferred to the respective state archive, except as otherwise may be provided by a special legislative instrument.

(3) Information may not be destroyed until one year after the expiration of the protection period.

(4) The State Information Security Commission shall authorise information to be destroyed, subject to the advice of a committee instituted by the order of the head of the appropriate organisational unit. Such committee shall:

1. give an opinion as to which information is of no historical, practical or a referential importance;

2. give an advice to destroy documents and materials.

(5) (Amended, SG No. 77/2018, effective 1.01.2019) The SISC decision to destroy information shall be appealable before the relevant Administrative Court under the procedure of the Code of Administrative Procedure.

(6) (New, SG No. 109/2008) Classified information obtained when using special intelligence means shall be destroyed pursuant to the provisions and as per the procedure of the Special Intelligence Means Act.

Section III

Protection Periods of Classified Information

Article 34

(1) The following shall be the protection periods of classified information, to commence from the date of generation:

1. of information marked as "Top Secret", 30 years;
2. of information marked as "Secret", 15 years;

3. of information marked as "Confidential", five years;

4. (amended, SG No. 95/2007) of information classified as an official secret, 6 months.

(2) Where national interest so requires, SISC may decide to extend the periods under paragraph 1, provided however that the extension shall not exceed the original protection period.

(3) Upon the expiration of the periods under paragraphs 1 and 2, the subject information shall be declassified and the access to such information shall be governed by the Access to Public Information Act.

(4) Where an organisational unit is completely abolished, its classified information which is a State secret or an official secret, and all its powers to modify the classification levels thereof, shall be transferred to SISC, except as otherwise may be provided by a special legislative instrument.

(5) The periods under paragraphs 1 and 2 shall apply as well to foreign classified information, except as otherwise may be provided by an international treaty to which the Republic of Bulgaria is a party.

Article 35

(1) The State Information Security Commission shall maintain a register of the materials and documents which contain classified information which is a State secret or an official secret.

(2) The register under paragraph 1 shall contain the following elements:

1. Organisational unit which generated the material or document.

2. Generation date and declassification date.

3. Identification number of the material or document under which it is entered on the register under paragraph 1.

4. Legal reasons for the classification of the material or document, and its security marking.

5. Modification of the classification level or declassification, and the date thereof.

(3) Upon generation of a material or document which contains classified information which is a State secret or an official secret, or upon modification of the classification level or the declassification thereof, as the case may be, the heads of organisational units shall provide the elements under paragraph 2, subparagraphs 1, 2, 4, and 5, to SISC for entry on the register.

(4) The persons under Article 31(1) shall, from time to time, but not less frequently than once in every two years, review the protection period of each material or document having a security marking for the existence of any legal reasons to modify its classification level or to declassify such material or document. In the event of modification of the classification level, the portion of the protection period under Article 34(1) prior to such modification shall be subtracted from the protection period corresponding to the new classification level.

(5) The procedure for the provision of the registration elements, and the conditions and procedure for retrieving information from the register, shall be laid down in the Detailed Rules for the Application hereof.

Chapter Five

ACCESS TO CLASSIFIED INFORMATION

Section I

Conditions for Access

Article 36

Except in the circumstances under Article 39, no person shall have a right of access to classified information merely by reason of official status.

Article 37

(1) The heads of organisational units, excepting those under paragraph 2, shall establish a list of the positions and assignments, and the respective classification levels, which require access to classified information which is a State secret.

(2) The heads of the security services and the public order of services shall establish the list under paragraph 1 for their respective services.

Article 38

(1) Access to classified information in connection with the performance of official duties or special assignments may not be allowed prior to:

1. the completion of a background investigation of the person to be allowed such access; and

2. the training of such person in the protection of classified information.

(2) No background investigation shall be conducted for the purposes of information classified as an official secret.

Article 39

(1) No background investigation shall be conducted of the following persons:

1. the Speaker of the National Assembly;

2. the President of the Republic of Bulgaria;

3. the Prime Minister;

4. (amended, SG No. 71/2016) the Deputy-Prime Ministers and the ministers;

5. the Chief Clerk of the Council of Ministers;

6. the Members of the National Assembly;

7. (supplemented, SG No. 55/2004, SG No. 62/2022) the Judges of the Constitutional Court, Judges, Prosecutors, European Public Prosecutor and European delegated prosecutors, Lawyers and Investigators;

8. (new, SG No. 28/2016, supplemented, SG No. 62/2016, effective 9.08.2016) the members of the Supreme Judicial Council, the chief inspector and the inspectors of the Inspectorate at the Supreme Judicial Council;

9. (new, SG No. 84/2023, effective 6.10.2023) the members of the Counter-Corruption Commission.

(2) The persons under paragraph 1, subparagraphs 1, 2 and 3, shall, effective from the assumption of office, have a right of access to all levels of classified information for the duration of their term in office.

(3) (Amended, SG No. 28/2016) The persons under paragraph 1, subparagraphs 4, 5, 6, 7 and 8, shall, effective from the assumption of office, have a right of access to all levels of classified information for the duration of their term in office in keeping with the "need-to-know" principle and, where the subject information is:

1. (amended, SG No. 71/2016) for the deputy-prime ministers, the ministers and the chief clerk of the Council of Ministers - within the scope of their competences;

2. for the Members of the National Assembly, subject to a decision, properly made, of a Parliamentary Committee or of the Assembly, or provided that such Committee or the Assembly

meets in a closed session;

3. (supplemented, SG No. 52/2004, SG No. 62/2022) for the Judges, Prosecutors, European Public Prosecutor and European delegated prosecutors, Lawyers and Investigators, for the purposes only of the case at hand;

4. (new, SG No. 28/2016) for the members of the Supreme Judicial Council – based on decision duly passed by the respective college or by the plenary of the Supreme Judicial Council, where the college or the plenary shall be sitting in camera;

5. (new, SG No. 62/2016, effective 9.08.2016) for the chief inspector and the inspectors of the Inspectorate at the Supreme Judicial Council – in the process of discharge of their duties.

Article 39a

(New, SG No. 89/2004)

(1) No reliability clearance shall be carried out in respect of persons upon or in relation to the exercise of their constitutional right to defense.

(2) Persons under para 1 shall ex lege have access to all levels of classified information for the time required for the exercise of their right to defence and in compliance with the "need to know" principle.

Article 40

(1) In no circumstance other than the ones under Article 39, shall a clearance for access to classified information be issued to any person, unless he meets the following requirements:

1. such person is a Bulgarian citizen, except in the circumstances under Chapter Six, Section VI; and

2. is of legal age; and

3. has completed secondary education; and

4. has not been convicted of premeditated felony, subsequent rehabilitation notwithstanding; and

5. (declared unconstitutional by Constitutional Court of the Republic of Bulgaria - SG No. 49/2016; repealed, SG No. 71/2016);

6. is reliable for the purposes of security; and

7. is not suffering from any mental disorder, as duly certified; and

8. is considered reliable for the purpose of protecting a secret.

(2) Where an international treaty exists to which the Republic of Bulgaria is a party, or on the basis of reciprocity, the requirements under paragraph 1 shall not apply to citizens of other States who, in the Republic of Bulgaria, perform such tasks as may be assigned to them by the State concerned or by an international organisation, provided that such persons shall have been cleared for access to classified information by the appropriate information security authority of such State or international organisation.

(3) (New, SG No. 103/2017, effective 1.01.2018) The circumstances under Item 4 of Paragraph 1 shall be established by official channels by the organisational unit initiating the procedure for background investigation of the relevant person for the purposes of access to classified information.

Article 41

A person shall be deemed to be reliable for the purposes of security in the absence of any data implicating such person:

1. in any activity directed against the interests of the Republic of Bulgaria or against any

interest which the Republic of Bulgaria has undertaken to safeguard in pursuance of international treaties;

2. as a participant in, or an accomplice to, any espionage, terrorist, sabotage or subversive activity;

3. in any other activity directed against the national security, the territorial integrity or the sovereignty of the Republic of Bulgaria or aimed at changing the constitutional order by the use of violence;

4. in any activity directed against public order.

Article 42

(1) A person shall be deemed reliable for the purpose of protecting a secret in the absence of any data to evidence:

1. any concealment of information or misrepresentation by such person for the purposes of the background investigation;

2. any facts or circumstances which might render such person vulnerable to blackmail;

3. a discrepancy between such person's living standard and his income;

4. a mental disorder or any other psychic disorder which might impair such person's capacity to operate with classified information;

5. such person's addiction to alcohol or psychotropic substances.

(2) For the purpose of establishing the facts under paragraph 1, subparagraphs 4 and 5, the investigating authority may require the person under investigation to undergo special medical and psychological tests and to present the results thereof. The person under investigation may refuse to undergo such tests. Such refusal shall be made in writing, and the background investigation shall be terminated.

(3) The procedure for, and the places of, the above special medical and psychological tests, as well as the periodical medical examinations under Article 18(1), subparagraph 4, and the methods thereof, shall be prescribed in a regulation by the Minister of Health, subject to consultation with SISC.

Section II

Background Investigation Procedure

Article 43

(1) The background investigation procedure shall have the purpose of establishing whether an applicant meets the requirements for clearance for access to classified information.

(2) (Supplemented, SG No. 71/2016) The background investigation procedure shall be conducted following written consent of the investigating person, including to conduct investigation for affiliation to the state security services and the intelligence service of the Bulgarian People's Army pursuant to the Access to and Disclosure of the Documents and Announcement of the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian People's Army Act.

(3) All such investigation activities shall be documented.

(4) The written consent under paragraph 2 may be withdrawn at any time during the investigation.

(5) In the event of such withdrawal, the person concerned shall not have a right to apply for appointment or for the performance of a special assignment, which requires access to classified

information, for a period of one year thereafter.

(6) In the circumstances under paragraph 4, the background investigation procedure shall be terminated immediately. Any materials or documents produced by the person under investigation shall be returned to him, and the data gathered in the course of the investigation shall be destroyed immediately by the investigating authority.

(7) The procedure for the purposes of paragraph 6 shall be laid down in the Detailed Rules for the Application hereof.

Article 44

(1) With a view to establishing the reliability of a person under background investigation for the purpose of protecting a secret, data shall be gathered in the course of such investigation about such third parties as the person under investigation shall specify in the appropriate questionnaire.

(2) (Repealed, SG No. 17/2019).

Article 45

(1) (Amended, SG No. 95/2007) The investigation under Article 43(1) shall be conducted for persons who occupy or apply to occupy a position or perform a task entailing access to classified information.

(2) The investigation under paragraph 1 shall be conducted also for persons whose work requires access to information classified at a higher level.

(3) The applicants in a competitive examination procedure for appointment or for the performance of a special assignment which requires access to classified information must meet the requirements hereunder for clearance for access to the appropriate level of classified information.

(4) The requirement under paragraph 3 shall be expressly cited in the announcement of the competitive examination.

(5) The specific requirements relating to the conduct of the investigation procedure for the persons under paragraph 3 shall be laid down in the Detailed Rules for the Application hereof.

Article 45a

(New, SG No. 71/2016)

(1) The investigation authority shall address a written request to the Commission for Disclosure of Documents and Announcement of the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian People's Army Act to conduct an investigation of the person under investigation pursuant to the Access and Disclosure of Documents and Announcement of the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian People's Army Act. Written consent of the investigated person to conduct the investigation shall be attached to the request. The commission shall conduct an investigation within a 14 days from receiving the request and shall send the result thereof to the investigating authority, and in case of established affiliation - also to the SISC and the investigated person.

(2) When affiliation has been established of the person under background investigation, the investigation authority, when it is different from the State Agency for National Security, shall send forthwith the entire file to the State Agency for National Security where the investigation shall be finalised.

(3) in the cases under Article 11, paragraph 1, item 1 and 2 and Article 15 when affiliation of the person under background investigation has been established, the investigation authority

shall conduct the investigation and shall send the entire file to the SISC to make a decision under Article 9, item 9a.

(4) The State Agency for National Security, the SISC respectively, in the cases under paragraph 3:

1. shall consider the facts and circumstances, contained in the results of the conducted background investigation under paragraph 1 in view of assessing whether the person subject to the investigation complies with the requirements under Article 40, paragraph 1;

2. may require additional information and copies of documents from the Commission for Disclosure of Documents and Announcement of the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian People's Army as well as from the person under investigation.

(5) In case of establishing affiliation the appeal against the decision of the Commission for Disclosure of Documents and Announcement of the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian People's Army shall not stop the investigation procedure under this Act.

(6) (Amended, SG No. 69/2020) No background investigation under paragraph 1 shall be conducted when the investigation authority is the State Intelligence Agency or the Military Intelligence Service of the Ministry of Defence.

Section III

Types of Background Investigation

Article 46

The following types of background investigation shall be conducted depending on the level of clearance required:

1. ordinary investigation, for access to information classified as "Confidential";
2. extensive investigation, for access to information classified as "Secret";
3. special investigation, for access to information classified as "Top Secret".

Article 47

(1) Ordinary investigation shall be conducted by the information security officer upon the written instructions of the head of the organisational unit.

(2) In the circumstances under Article 20 (3), such investigation shall be conducted by the head of the organisational unit.

(3) (Amended, SG No. 71/2016) Ordinary investigation shall be conducted for the purpose of establishing the facts and circumstances under Article 40 (1), Items 1 – 4, 7 and 8.

(4) The investigation under paragraph 1 shall include the completion of a questionnaire (Schedule 2).

(5) To verify the facts and circumstances under paragraph 4, the information security officer shall have a right to require and to receive data from the public order services and from the competent government authorities, and, as necessary, shall have a right to require assistance from the security services.

(6) The information security officer shall conclude the investigation and shall issue or deny clearance for access to information which is a State secret and is classified as "Confidential", and shall promptly advise SISC.

Article 48

(1) Extensive investigation shall be conducted for persons who apply for appointment or for the performance of a special assignment which requires operation with information classified as "Secret".

(2) (Amended, SG No. 109/2007) The investigation under paragraph 1 shall be conducted, except in the circumstances under Articles 11 and 15, by the State Agency for National Security at the written request of the head of the organisational unit to which the person concerned applies for appointment or which issues a special assignment.

(3) The investigation under paragraph 1 shall be conducted for the purpose of establishing the facts and circumstances under Article 40(1).

(4) The investigation under paragraph 1 shall include the completion of a questionnaire (Schedule 2).

(5) (Amended, SG No. 31/2003, SG No. 109/2007) The extensive investigation shall, in addition to establishing and verifying the facts and circumstances under paragraphs 3 and 4, include verifications at the domicile and the place of work, and of the bank accounts of the person under investigation, and in the tax registers.

Article 49

(1) Special investigation shall be conducted for persons who apply for appointment or for the performance of a special assignment which requires operation with information classified as "Top Secret".

(2) (Amended, SG No. 109/2007) The investigation under paragraph 1 shall be conducted, except in the circumstances under Articles 11 and 15, by the State Agency for National Security at the written request of the head of the organisational unit to which the person concerned applies for appointment or which issues a special assignment.

(3) The special investigation shall include the activities under Article 48, paragraphs 3-5, and an interview with the person under investigation and with three other persons, such as the person under investigation shall specify.

Article 50

(1) If any facts and circumstances are revealed in the course of the examination under Articles 47, 48 or 49, such as present an impediment to the issuance of the appropriate level clearance, there shall be conducted an additional interview with the person under investigation.

(2) The interview under paragraph 1 shall be conducted for the purpose of obtaining greater clarity on the facts and circumstances so revealed.

(3) Such interview shall be conducted, depending on the type of investigation under way, by:

1. where an ordinary investigation, the information security officer or, as the case may be under Article 20(3), the head of the organisational unit;

2. where an extensive or a special investigation, the appropriate investigating authority.

(4) No interview under paragraph 1 shall be conducted where, were it to be conducted, such interview might entail an unauthorised access to information which is a State secret.

Article 51

(Amended, SG No. 35/2009, effective 12.05.2009)

Within the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army, the investigation under Articles 47(1), 48(1) and 49(1) shall be

conducted by the authority under Article 11(3) at the written request of the head of the appropriate structural unit.

Section IV

Time Limits for Investigation and Issuance or Denial of Clearance

Article 52

(1) The background investigation shall be completed within the following time limits:

1. of an ordinary investigation, 30 days from the date of receipt of the relevant instructions or request;

2. of an extensive investigation, 45 days from the date of receipt of the relevant written request of the head of the organisational unit;

3. of a special investigation, 60 days from the date of receipt of the relevant written request of the head of the organisational unit.

(2) The appropriate heads of units may extend the time limits under paragraph 1, but by not more than 20 days, on the basis of the written reasoned request of the officers of the security or the public order services, or of the information security officers, conducting the investigation, provided however that such request shall be made prior to the expiration of the original time limit.

(3) (New, SG No. 71/2016) In case of establishing affiliation under article 45a the deadlines under paragraph 1 shall be extended by 15 days.

Article 53

The State Information Security Commission, the services under Articles 11 and 15 or the information security officer shall issue or deny clearance for access to information classified at the appropriate level within 10 days from the date of completion of the background investigation.

Section V

Issuance, Revocation, Termination, and Denial of Clearance for Access the Classified Information

Article 54

(1) Clearance for access shall be issued to such persons as meet the requirements under Article 40(1) for the appropriate classification level.

(2) The clearance for access is a document made in writing. Its shall be issued in triplicate, on such sample form as SISC shall approve, to be kept, one each, by SISC, the issuing service, and the appropriate organisational unit.

(3) The clearance for access to any higher classification level shall entitle the holder thereof to access to information classified at a lower level if the latter is required by the holder's official position or performance of a special assignment.

Article 55

(1) Clearance for access shall be issued for a period of:

1. five years, to information classified as "Confidential";
2. four years, to information classified as "Secret";
3. three years, to information classified as "Top Secret".

(2) Not later than three months before the expiration of a period under paragraph 1, a new background investigation shall be conducted of the persons who continue in a position, or with the performance of a special assignment, which requires access to information classified at the appropriate level.

(3) The investigation under paragraph 2 and the issuance of a new clearance shall be done by the competent authorities under the conditions and procedure provided for in this Chapter.

(4) (New, SG No. 95/2007) No new background investigation shall be conducted with regard to a person who, within the period of validity of the issued clearance for access, moves to a different position or needs to perform a different task requiring access to classified information of the same or a lower information security level as compared to the level for which the person has been cleared.

Article 56

(1) Where, concerning a person cleared for access to classified information, new facts and circumstances are revealed which raise a doubt as to such person's reliability, the security information officer shall inquire into such facts and circumstances.

(2) The inquiry under paragraph 1 shall be conducted immediately and for the purpose of obtaining greater clarity on the said facts and circumstances.

(3) The security information officer shall advise such inquiry in writing to the head of the organisational unit and the authority which issued the clearance.

(4) Upon such advice, the head of the organisational unit may restrict the access of the person under inquiry to the appropriate classification level and shall immediately advise the issuing authority.

Article 57

(1) Clearance for access to classified information of the appropriate level shall be denied where it is established, in the course of a background investigation, that:

1. the person under investigation does not meet any one of the requirements under Article 40(1);

2. the person under investigation has deliberately misrepresented or withheld any facts and circumstances.

(2) The denial of clearance shall be issued in triplicate, on such sample form as SISC shall approve, to be kept, one each, by SISC, the issuing authority, and the appropriate organisational unit.

(3) The denial of clearance shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for denial.

(4) The person under investigation shall be notified of such denial in writing, setting out the legal reasons for denial, and shall be issued with a transcript thereof.

(5) (Repealed, SG No. 71/2016).

(6) No person under investigation who is denied clearance for access to classified information shall have a right to apply for appointment or for the performance of a special assignment, such as requires access to information classified at the same or at a higher level, for a period of one year from the date of such denial.

Article 58

The clearance, and the denial of clearance, for access to classified information shall set out:

1. The issuing authority;
2. The full name, the date and place of birth, and the Personal Identity Number of the person under investigation;
3. (Repealed, SG No. 95/2007);
4. The type of investigation;
5. The level of classification to which access is cleared or denied;
6. The legal reasons for clearance or the denial thereof;
7. The document's term of validity;
8. The document's number;
9. The document's date and place of issuance;
10. Signature and stamp.

Article 59

(1) (Amended, SG No. 71/2016) The body that has issued the clearance for access to classified information shall revoke the issued clearance when:

1. (amended, SG No. 71/2016) it is established that the person concerned does not meet any one of the requirements under Article 40, paragraph 1;

2. the person concerned has committed an offence under any of the provisions of this Act or of the implementing statutory instruments hereto, and has thereby threatened or caused grave damage to the interests of the State or of the organisations or persons concerned with the protection of classified information;

3. the person concerned has committed systematic offences under this Act or any statutory instrument relating to the protection of classified information.

(2) The authority under paragraph 1 shall immediately advise the revocation of clearance in writing to the appropriate head of organisational unit and to the person concerned.

(3) The revocation of clearance shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for revocation.

(4) The revocation of clearance shall be based on a written statement containing the appropriate elements under Article 58.

(5) (Repealed, SG No. 71/2016).

(6) No person whose clearance for access to classified information is revoked shall have a right to apply for appointment or for the performance of a special assignment, such as requires access to classified information, for a period of three years from the date of such revocation.

Article 60

(1) The issuing authority of a clearance for access to classified information shall terminate such clearance, subject to the advice, made in writing, of the appropriate information security officer, in the event of:

1. the death of the holder of such clearance;
2. (repealed, SG No. 95/2007);
3. (repealed, SG No. 95/2007);
4. expiration of the appropriate period under Article 55(1);
5. change in the need for access to information classified at a higher level;

6. (new, SG No. 95/2007) ceased need to access classified information.

(2) The authority under paragraph 1 shall advise the termination of clearance in writing to the appropriate head of organisational unit and to the person concerned.

(3) The termination of clearance shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for termination.

(4) The termination of clearance shall be based on a written statement containing the appropriate elements under Article 58.

(5) (Repealed, SG No. 71/2016).

Article 61

In the circumstances under Articles 59 or 60, the officer concerned shall return the clearance to the issuing authority.

Article 62

A denial of clearance for access to classified information, and the termination or revocation thereof, may be appealed before SISC within seven days from the date of advice to the person concerned under Article 57(4) or 59(2) or 60(2), as the case may be.

Article 63

(1) Such appeal shall be made in writing and addressed to SISC in the care of the authority whose act is the subject thereof.

(2) The appeal shall set out the authority before which it is laid; the name and address of the appellant; the act which is the subject of appeal; the authority which issued such act; the appellant's complaint and petition.

Article 64

(1) Any appeal laid after the period under Article 62 shall be returned to the appellant against his acknowledgement of receipt.

(2) Within seven days of return, a request may be made for renewal of the period for appeal, provided that the original period was not complied with on account of special unforeseen circumstances. The original appeal so returned shall be attached to such request.

(3) The request for renewal of the period for appeal shall be considered by SISC. If such request is deemed to be valid, the appeal shall be admitted, and if not, the appeal shall be dismissed without a hearing.

Article 65

(1) Within seven days from the date of receipt of an appeal, the authority which issued the subject act may reconsider the matter and may issue clearance for access to classified information or, as the case may be, withdraw the act whereby clearance had been revoked. The person concerned shall be advised accordingly.

(2) If the authority which issued the subject act does not find any reason to reverse its decision, it shall immediately refer the appeal, together with all the relevant documents, to SISC.

(3) If, within seven days from the expiration of the time limit under paragraph 1, the appeal has not been referred to SISC, the appellant may send a transcript thereof to SISC or advise SISC of the delay. SISC shall require delivery of the relevant documents ex officio.

(4) After receipt of the relevant documents, SISC may gather new evidence.

Article 66

(1) The State Information Security Commission shall adjudicate on the appeal within two weeks from the date of receipt thereof.

(2) The State Information Security Commission shall adjudicate by a ruling whereby it shall revoke the administrative act of denial, termination or revocation of clearance, as the case may be, or dismiss the appeal.

(3) Where the authority concerned had unlawfully denied clearance for access to classified information, SISC may direct the authority to commence a background investigation procedure, to be completed within such time as SISC shall prescribe.

Article 67

Within three days from the date of the ruling, SISC shall announce it to the appellant, to the authority which issued the subject act, and to the appropriate organisational unit.

Article 68

(Amended, SG No. 71/2016)

(1) The decision of the SISC shall be subject to appeal before a three-judge panel of the Supreme Administrative Court.

(2) The appeal shall be lodged within 14 days with the Supreme Administrative Court which shall rule within one month and its ruling shall be final.

(3) The appeal shall not stop the execution and shall be considered in camera under the procedure of Chapter Twelve of the Administrative Procedure Code.

(4) Access to the file in the court registry and in the courtroom shall be provided to the parties, their proxies and to the persons, to whom the Chairperson of the court allows this.

Article 69

(Amended and supplemented, SG No. 71/2016)

The denial, termination and revocation of an issued clearance for access to classified information issued by the SISC shall be subject to appeal before a three-judge panel of the Supreme Administrative Court. The ruling of the court shall be final.

Section VI

Background Investigation Files

Article 70

(1) The files of materials relating to background investigations shall be kept, maintained, updated, card-filed, and closed by the investigating authority, separately from other files.

(2) Such file shall be opened by the competent authority upon the commencement of a background investigation.

(3) (Amended, SG No. 95/2007) The data contained in such file is classified information and may only be used for the purposes of this Act.

(4) The files of persons who have been cleared for access to classified information shall be kept for a period not to exceed five years after the expiration of the clearance period, whereafter, such files shall be destroyed.

Article 71

(1) The file of a person under investigation shall contain:

1. The application for appointment or the documents relating to a special assignment, which requires access to classified information, or as the case may be, the application for a competitive examination for the purposes of such appointment or special assignment.

2. The documents relating to a natural or legal person proposing to enter or perform a contract involving access to classified information.

3. The person's written consent to the background investigation.

4. The written request for background investigation.

5. The completed investigation questionnaire.

6. The clearance, certificate, or certifying document for access to classified information.

7. The document of denial, revocation, or termination of the clearance for access to classified information.

8. The documents of appointment or special assignment.

9. The documents relating to the completion of training in the protection of classified information.

10. Any other documents evidencing facts and circumstances established in pursuance of this Act.

(2) The special rules for the opening, the storing, the maintenance, the updating, the card-filing, and the closing of background investigation files shall be laid down in the Detailed Rules for the Application hereof.

Chapter Six

TYPES OF CLASSIFIED INFORMATION PROTECTION

Section I

Physical Security

Article 72

(1) The physical security of classified information includes a system of organisational, physical, and technical measures for the prevention of unauthorised access to materials, documents, equipment, and facilities classified as a State secret or an official secret.

(2) The system of measures under paragraph 1 includes the protection of the buildings, the premises, and facilities within or at which classified information is generated, processed, or stored, and the control of access to such buildings, premises, and facilities.

Article 73

(1) The organisational units shall apply a system of measures and devices for the physical security of the buildings, the premises, or the facilities within or at which classified information is generated, processed, or stored.

(2) Physical security shall be used for the protection of classified information from any threat or damage resulting from:

1. terrorist activities or sabotage; or

2. unauthorised access or attempted unauthorised access.

(3) The necessary techniques and devices for physical security shall be determined in accordance with the classification level and the volume of classified information, the number and

the clearance levels of staff, as determined pursuant to Article 3, and the level of threat of any damaging action.

Article 74

To prevent unauthorised access to classified information, the heads of organisational units, with the assistance of the information security officer, shall:

1. define security perimeters;
2. around the security perimeters, define administrative perimeters of the lowest security level within which persons and vehicles shall be controlled;
3. introduce a control arrangement for entry into, movement within, and exit from, the security perimeters, and for the escorting within such perimeters of the visitors not cleared for access to classified information or cleared for access to information classified at a lower level than the one held within the security perimeter;
4. provide the appropriate control of the security and the administrative perimeters with the support of the appropriate security units;
5. introduce a special arrangement for the safekeeping of keys to the premises, safes and other facilities used for storing classified information.

Article 75

To protect classified information which is a State secret in the course of meetings, talks, conferences, etc, of which such information is the subject, additional security measures shall be introduced to prevent bugging or unauthorised observation.

Article 76

The persons participating in meetings or conferences, of which classified information which is a State secret is the subject, shall undergo a prior security check by the security unit of the organisational unit.

Article 77

(1) All materials and technical devices used for the protection of classified information must conform to the durability and indestructibility requirements appropriate to each classification level, as certified by SISC or by another authority designated by the Council of Ministers.

(2) Any technical devices other than the above may not be used otherwise than by way of an exception and provided that the appropriate security level shall not be compromised.

(3) The physical security measures, as certified for each classification level, shall be described in a schedule which SISC shall approve.

Article 78

The system of physical security measures, techniques, and devices, and the conditions and procedure for the operation thereof, shall be laid down in a regulation by the Council of Ministers.

Article 79

The information security officers shall exercise ex ante and current control over the physical security arrangements, techniques, and devices at their respective organisational unit.

Section II

Documentary Security

Article 80

(1) Documentary security is a system of measures, techniques, and devices for the protection of classified information during the preparation, the processing, and the storing of documents, and in the organisation and operation of classified information registries.

(2) The system of documentary protection measures, techniques, and devices, and the conditions and procedure for the operation thereof, shall be laid down in the Detailed Rules for the Application hereof.

Article 81

To ensure the protection of classified information, the heads of organisational units shall, within their terms of reference, establish additional special procedures and requirements.

Article 82

(1) Within each organisational unit, there shall be created a separate classified information registry which shall be responsible for the proper preparation, processing, and storing, and delivery to the authorised persons of materials which contain classified information. Such classified information registry shall report directly to the appropriate information security officer.

(2) Requirements relating to the organisation and operation of the registries under paragraph 1 shall be laid down in the Detailed Rules for the Application hereof.

Section III Personal Security

Article 83

(1) Personal security is a system of such principles and measures as the competent authorities, following the appropriate procedure, shall apply to persons with a view to ensuring such persons' reliability for the purposes of protecting classified information.

(2) The principles and measures under paragraph 1 include the "need to- know" principle, the background investigation procedure, and the issuance of access clearance under Chapter Five, the training of persons pursuant to this Act and the Detailed Rules for the Application hereof, and the exercise of control in these areas.

Section IV Cryptographic Security

Article 84

Cryptographic security is a system of cryptographic methods and devices used to protect classified information from unauthorised access during the generation, the processing, the storing, and the transmission of such information.

Article 85

(Amended, SG No. 109/2007)

The conditions and procedure for the manufacture and import of cryptographic methods and

devices for the protection of classified information shall be laid down in a regulation by the Council of Ministers, subject to the advice of the Chairperson of the State Agency for National Security.

Article 86

(Amended, SG No. 109/2007)

No cryptographic method or device shall be used for the protection of classified information prior to the approval and registration of such method or device by the State Agency for National Security.

Article 87

(1) (Amended, SG No. 109/2007) The generation and distribution of the necessary cryptographic keys shall be the responsibility of the State Agency for National Security.

(2) (Amended, SG No. 109/2007) The activities under paragraph 1 may be performed as well by any other organisational unit, subject to the prior approval, and under the control of the State Agency for National Security.

Article 88

(1) Within each organisational unit, the use of cryptographic methods and devices shall be the responsibility of the information security officer, or of such other officers of the administrative security unit who have been trained in the field of cryptographic security and have been authorised to use cryptographic devices.

(2) (Amended, SG No. 109/2007, supplemented, SG No. 71/2016) The authorisation under paragraph 1 shall be issued by the State Agency for National Security, subject to prior background investigation under Article 46, paragraph 3. The issuance, termination or revocation of such authorisation shall be governed by the provisions of Chapter Five. The denial, termination or revocation of such authorisation shall not be appealable before the courts of law. They shall be subject to appeal before SISC under the procedure in Articles 62 - 67.

(3) (Amended, SG No. 109/2007) The training under paragraph 1 shall be administered by the State Agency for National Security, or by any other organisational unit, subject to the prior approval, and under the control of the said Directorate.

Section V

Security of Communication and Information Systems

(Title amended, SG No. 88/2018)

Article 89

(Amended, SG No. 88/2018)

The security of communication and information systems (CIS) is a system of principles and measures for the protection from unauthorised access of such classified information as is generated, processed, stored, or transmitted by CIS.

Article 90

(Amended, SG No. 109/2007, SG No. 36/2008, SG No. 88/2018)

(1) The general required conditions for the security of CIS include computer security,

communications security, cryptographic security, physical security, document security and personal security, CIS connection security, the security of information as such on any electronic medium, and TEMPEST countermeasures, as defined in a regulation proposed by the Chairperson of the State Agency for National Security and adopted by the Council of Ministers.

(2) Each CIS shall be subjected to a security risk analysis in accordance with the requirements laid down in the regulation referred to in Paragraph 1.

(3) The specific requirements for the security of CIS within each organisational unit shall be proposed by the information security officer and established by the head of such unit. These requirements and procedures shall be adopted subject to the approval of the State Agency for National Security.

(4) The requirements and procedures under Paragraph 3 shall include a detailed description of the security measures and rules applied to the design and operation of the CIS concerned.

(5) The requirements and procedures under paragraph 3 shall be drawn up subject to the conditions and procedure laid down in the regulation referred to in Paragraph 1.

(6) Any subsequent changes in the specific security requirements and procedures under Paragraph 3 shall be subject to endorsement by the State Agency for National Security subject to the conditions and procedure laid down in the regulation referred to in Paragraph 1.

Article 91

(Amended, SG No. 109/2007, SG No. 88/2018)

(1) Upon the commissioning of any CIS to operate with classified information, an accreditation procedure shall be conducted in accordance with the conditions and procedure laid down in the regulation referred to in Article 90, Paragraph 1.

(2) No classified information may be generated, processed, stored, or transmitted in a CIS in the absence of a certificate issued under Article 14, Item 2.

Article 92

(Amended, SG No. 88/2018)

The head of an organisational unit which operates any CIS shall, as proposed by the information security officer, appoint employees or assign to existing employees to perform control functions concerning the security compliance of such CIS in accordance with the conditions and procedure laid down in the regulation referred to in Article 90, Paragraph 1.

Article 93

(Amended, SG No. 88/2018)

(1) In case that systematic offences of the requirements on the security of classified information generated, processed, stored, or transmitted by CIS are established, the State Agency for National Security shall revoke the certificate issued under Article 14, item 2 as proposed in writing by the authority responsible for the direct control over the protection of classified information.

(2) The State Agency for National Security shall terminate the certificate issued under

Article 14, item 2:

1. upon the expiry of the period of validity of the security certificate issued to the CIS concerned;
2. in the event of removal or alteration of the level of classification of the information generated, processed, stored, or transmitted by CIS;
3. upon the decommissioning of the CIS concerned;
4. upon the closing down of the organisational unit without a successor.

(3) The withdrawal or termination of a certificate issued as provided for by Article 14, Item 2 may be appealed against before the SISC subject to the conditions and procedure and within the time limit laid down in Chapter Five, Section V, and may not be appealed against in court.

Article 94

(Amended, SG No. 88/2018)

(1) CIS designed for classified information up to and including the "Secret" level may be interconnected with other CIS for classified information of the same or a different level of classification and with closed-type information systems subject to the conditions laid down in the regulation referred to in Article 90, Paragraph 1.

(2) CIS designed for classified information of the "For Official Use Only" level may be interconnected with the internet or other public networks subject to the conditions laid down in the regulation referred to in Article 90, Paragraph 1.

(3) CIS designed for classified information of the "Confidential" and "Secret" levels may not be interconnected with CIS designed for classified information of the "For Official Use Only" level which are connected to the internet or other public networks.

(4) CIS designed for classified information of the "Top Secret" level may not be interconnected.

Article 94a

(New, SG No. 103/2012, amended, SG No. 88/2018)

Interconnection shall only be allowed where:

1. Network border protection mechanisms are put in place in the CIS which have been approved by the State Agency for National Security, subject to the conditions and procedure laid down in the regulation referred to in Article 90, Paragraph 1;

2. A valid security certificate issued under Article 14, Item 2 is in place for the communication and information systems concerned.

Article 94b

(New, SG No.103/2012, repealed, SG No. 88/2018).

Article 94c

(New, SG No. 103/2012, amended, SG No. 71/2016, repealed, SG No. 88/2018).

Section VI

Industrial Security

Article 95

(1) Industrial security is a system of principles and measures applied to persons, whether natural or legal, who propose to enter or perform a contract which involves access to classified information, for the purposes of protecting such information from unauthorised access.

(2) The general industrial security requirements shall be defined pursuant to this Act in a regulation by the Council of Ministers.

(3) Subject to the advice of SISC, the Council of Ministers shall designate an authority to perform background investigations and issue security certificates.

(4) The contract under paragraph 1 shall provide specific requirements for the protection of classified information, relating in particular to the volume and level of classified information, the persons allowed access thereto, and the liability for non-compliance with the industrial security requirements.

Article 96

(1) Classified information may not be disclosed to any natural person, unless such person is certified and cleared for access to such information, nor to any legal person, unless such person is certified for such access.

(2) In circumstances other than those under paragraph 1, where there are reasons to believe that, in the course of operation, a person may generate or receive access to classified information, such person shall have a duty to request clearance under Chapter Five or certificate under this Section.

Article 97

(1) For the purposes of certification, the bidder shall undergo background investigation whereby data shall be gathered about:

1. the bidder's management personnel, and the persons immediately involved in the performance of the contract under Article 95(1);
2. the persons involved in the negotiations on the contract under Article 95(1);
3. the bidder's administrative security unit personnel.

(2) For the purposes of such background investigation, data shall be gathered also about:

1. the bidder's structure and origin of capital;
2. the bidder's commercial partners, financial relations, real rights, etc, as necessary to assess the bidder's reliability.

Article 98

(1) For the purposes of the above background investigation, the bidder shall complete a questionnaire, as defined in the Detailed Rules for the Application hereof.

(2) In the event of any subsequent change in the data entered in the questionnaire under paragraph 1, the bidder shall have a duty to advise immediately the investigating authority.

Article 99

A bidder which misrepresents data, or provides incomplete data, for the purposes of the questionnaire under Article 98(1) shall not be certified for access to classified information.

Article 100

No bidder shall be certified for access the classified information, unless such bidder:

1. meets the security requirements under this Act and the implementing statutory instruments hereto;
2. is economically stable;
3. is reliable for the purposes of security.

Article 101

(1) No bidder shall be deemed to be economically stable if such bidder:

1. has been declared bankrupt or is in pending bankruptcy proceedings;
2. has been convicted of fraudulent bankruptcy;
3. is in liquidation;
4. has been barred from carrying on commercial activities;
5. has a liability, liquid, due and payable, to the Treasury or to any social security fund or to any natural or legal person, where such liability has been accepted before the authority of writ or has been established by an effective judgment or by a notarised document or security issued by a third party;
6. has been convicted of, and effectively sentenced for, a crime against property or the economy, unless subsequently rehabilitated.

(2) The requirement under paragraph 1, subparagraph 6, shall apply also to the bidder's managers or, as the case may be, members of governance.

(3) (Supplemented, SG No. 105/2020, effective 1.01.2021) The circumstances under Paragraph 1 shall be certified with a document by the respective competent authority, with the exception of the information for the existence or the absence of public obligations for the candidates, which shall be established under the procedure of Article 87, Paragraph 11 of the Tax and Social Insurance Procedure Code.

Article 102

(1) No bidder shall be deemed to be reliable for the purposes of security if:

1. such bidder is found, on the basis of data, not to meet the requirements under Article 41;
2. any of the persons nominated by the bidder for background investigation are found not to meet the security requirements under Article 40.

(2) In the circumstances under paragraph 1, subparagraph 2, the bidder may nominate substitute persons.

(3) The bidder's background investigation for the purposes of paragraph 1 shall be conducted by the security services.

Article 103

(1) Based on the result of the background investigation, the investigating authority shall either issue or deny security certificate.

(2) Security certificate shall be denied where the bidder does not meet therequirements under Article 100.

(3) The denial under paragraph 2 shall not be accompanied with an explanation of reasons and shall only set out the legal reasons for denial.

Article 104

(1) Security certificates and denials to issue such certificates shall be issued on such sample form as SISC shall approve, and shall set out:

1. The competent authority.
2. The name, the registered office, and the BULSTAT Number of the bidder who is issued or denied certificate.
3. The legal reasons for issuance or denial.
4. The number of the certificate or denial.
5. The certificate's term of validity.
6. The date and place of issuance or denial.
7. The signature and stamp of the issuing authority.

(2) The certificate, and the denial thereof, are written documents and shall be issued in triplicate, to be kept, one each, by SISC, the investigating authority, and the bidder.

Article 105

The head of the organisational unit which is the principal under the contract shall designate a person to exercise control of compliance with the provisions of this Act and the implementing statutory instruments hereto, and to consult the contractor during contract performance.

Article 106

(Amended, SG No. 95/2007)

(1) The security certificate shall be issued for no more than three years.

(2) No new investigation shall be conducted for natural or legal persons who, within the period of validity of the issued security certificate, propose to perform another contract which involves access to classified information of the same or a lower information security level as compared to the level for which the security certificate has been obtained.

Article 107

(Amended, SG No. 95/2007)

(1) If necessary, at least three months prior to the expiration of the issued security certificate, a new investigation shall be conducted regarding the natural or legal person, if such person continues to perform the same or another contract requiring access to classified information.

(2) The investigation under paragraph 1 and the issuance of a new security certificate shall be performed by the relevant competent authority under Article 95, paragraph 3 under the conditions and procedure laid down in this Section.

Article 108

(1) The authority which issued the certificate shall exercise control to ensure that the contractor is currently in compliance with the security requirements hereunder.

(2) Where the holder of a security certificate no longer meets the requirements under Article 100(1), the issuing authority shall prescribe a time limit for the removal of irregularities, provided that these have not already resulted in unauthorised access to classified information.

(3) Where the holder of a security certificate no longer meets any of the requirements under Article 100(2) or (3), and has failed to remove the irregularities within the time limit under paragraph 2, or it has been established that the irregularity under Article 100(1) has resulted in unauthorised access to classified information, the security certificate shall be revoked by the

issuing authority.

Article 109

(Amended, SG No. 71/2016)

The denial under Article 103(2) and the revocation of security certificate shall not be appealable before the courts of law, but shall be subject to appeal before SISC under the procedure in Articles 62 - 67.

Article 110

(1) The data gathered in the course of background investigations pursuant to this Section shall be kept by the appropriate investigation authority in a separate file and shall be protected as classified information.

(2) The data contained in the files under paragraph 1 may be used for the purposes of this Act.

(3) The files under paragraph 1 shall be kept for a period of 20 years commencing with the date of termination of the contractor's activities.

(4) The special rules for the opening, the storing, the maintenance, the updating, the card-filing, and the closing of background investigation files shall be laid down in the Detailed Rules for the Application hereof.

Article 111

The protection of classified information in the field of inventions and utility models shall be ensured in accordance with the provisions of the Patents Act, except as otherwise may be provided hereunder.

Article 112

The persons under Article 95(1), having been issued with security certificate in pursuance of this Section, shall have all the duties of organisational units hereunder.

Chapter Seven

DISCLOSURE OR EXCHANGE OF CLASSIFIED INFORMATION BY THE REPUBLIC OF BULGARIA TO, OR WITH, ANOTHER STATE OR AN INTERNATIONAL ORGANISATION

Article 113

(1) The Republic of Bulgaria discloses or exchanges classified information to, or with, States or international organisations where international treaties on the protection of such information exist between the Republic of Bulgaria and such States or international organisations.

(2) Where an international treaty under paragraph 1 does not provide for the applicable law with regard to any matters not provided for thereunder, the applicable law shall be that of the party of information source.

(3) (New, SG No. 17/2018, effective 23.02.2018) Where no international treaties on the protection of classified information exist between the Republic of Bulgaria and another State or

an international organisation, the Republic of Bulgaria shall disclose to or exchange classified information with such State or international organisation only in the cases relating to the protection of national security.

(4) (New, SG No. 17/2018, effective 23.02.2018) Paragraph 3 shall apply to classified information of the Republic of Bulgaria with security level "For Official Use Only", "Confidential" and "Secret".

(5) (New, SG No. 17/2018, effective 23.02.2018) Paragraph 3 shall not apply to foreign classified information provided to the Republic of Bulgaria by another state or an international organisation.

(6) (New, SG No. 17/2018, effective 23.02.2018) Disclosure or exchange under paragraph 3 shall be carried out only where prior written confirmation by the respective State or international organisation exists that the legislation and the system in place for protection of classified information ensure for the disclosed classified information a degree of protection which is the same or a higher than that provided for in this Act, including the respective liability in the case of violation of the rules for its protection.

(9) (New, SG No. 17/2018, effective 23.02.2018) The written confirmation under paragraph 6 shall be provided by the relevant competent authority for security of the other State or the international organisation.

Article 114

(1) (Previous text of Article 114, SG No. 17/2018, effective 23.02.2018) The decision to disclose or exchange information in pursuance of Article 113(1) shall be made by SISC on the basis of the preliminary opinion of the organisational unit which releases such information.

(2) (New, SG No. 17/2018, effective 23.02.2018) The decision to disclose or exchange information in pursuance of Article 113(3) shall be made by SISC on a case-by-case basis, based on a preliminary written reasoned opinion of the organisational unit which releases such information.

(3) (New, SG No. 17/2018, effective 23.02.2018) The reasoned opinion under paragraph 2 must specify the State or the international organisation to which classified information needs to be disclosed, the need and the specific interests relating to national security that must be protected, as well as the information security level of the information.

Article 115

(1) In accordance with the relevant international treaty, SISC and the competent information security authority of the other State or of the international organisation must, on a reciprocal basis and prior to the disclosure or exchange of information, ensure that such information will be properly protected.

(2) For the purposes of paragraph 1, the competent information security authority of the other State or of the international organisation must certify before SISC that the persons who will have access to the information disclosed or exchanged are duly cleared for access to information classified at the appropriate or at a higher level.

Article 116

With respect to classified information exchanged with, or disclosed to, the Republic of Bulgaria by an international organisation of which the Republic of Bulgaria is a member, such protection of classified information principles, norms, and procedures shall apply, as exist within such international organisation, if such an obligation derives from the Republic of Bulgaria's

membership of such organisation.

Chapter Eight

ADMINISTRATIVE PENALTIES

Article 117

(1) Whoever commits an offence under Article 17 shall be liable to a fine from BGN 2,000 to 20,000.

(2) Where an offence under Article 17 has been committed by a legal person, such person shall be liable to pay damages from BGN 2,000 to 20,000.

(3) For failure to prevent an offence under paragraph 2, a legal person's chief executive shall be liable to a fine from BGN 1,000 to 5,000, unless the offence is a criminal one.

Article 118

(1) Whoever commits an offence under Articles 18 and 19 shall be liable to a fine from BGN 50 to 300.

(2) The fine under paragraph 1 shall be imposed also on any head of organisational unit or any information security officer who fails to prevent an offence under Articles 18 and 19.

Article 119

Any information security officer who commits an offence under Article 22 shall be liable to a fine from BGN 100 to 1,000.

Article 120

(1) Whoever commits an offence under Article 31 shall be liable to a fine from BGN 100 to 500.

(2) The fine under paragraph 1 shall be imposed also on any head of organisational unit or any information security officer who fails to prevent an offence under Article 31.

Article 121

Any person under Article 31(1) who commits an offence under Article 35(4) shall be liable to a fine from BGN 100 to 1,000.

Article 122

(1) Any official person who commits an offence under Article 43(6) shall be liable to a fine from BGN 50 to 5,000, unless the offence is a criminal one.

(2) The fine under paragraph 1 shall be imposed also on any head of organisational unit or any information security officer who fails to prevent an offence under Article 43(6).

Article 123

Any head of organisational unit or information security officer who commits or fails to prevent an offence under Article 73(1) shall be liable to a fine from BGN 50 to 400.

Article 124

(1) Whoever commits an offence under Article 86 shall be liable to a fine from BGN 2,000 to 10,000.

(2) Where an offence under Article 86 has been committed by a legal person in the course of its operations, such person shall be liable to pay damages from BGN 3,000 to 15,000.

(3) For failure to prevent an offence under paragraph 1, a legal person's chief executive shall be liable to a fine from BGN 300 to 2,000.

Article 125

(Amended, SG No. 88/2018)

Any head of organisational unit who commits or fails to prevent an offence under Article 90(3), second sentence, shall be liable to a fine from BGN 300 to 2000.

Article 126

Any head of organisational unit who commits or fails to prevent an offence under Article 92 shall be liable to a fine from BGN 500 to 1,000.

Article 127

(1) (Amended, SG No. 88/2018) Whoever commits or fails to prevent an offence under Article 91(2) and Article 94 shall be liable to a fine from BGN 500 to 1000.

(2) (Amended, SG No. 88/2018) Any head of organisational unit who fails to prevent an offence under Article 91(2) and Article 94 shall be liable to a fine from BGN 1000 to 2000.

Article 128

(1) Whoever commits an offence under Article 96 shall be liable to a fine from BGN 1,000 to 3,000.

(2) Any legal person who commits an offence under paragraph 1 shall be liable to pay damages from BGN 1,000 to 5,000.

(3) Any head of organisational unit or information security officer who commits or fails to prevent an offence under Article 96 shall be liable to the fine from BGN 500 to 1,000, unless the offence is a criminal one.

Article 129

(1) Whoever commits or fails to prevent an offence under Article 98(2) shall be liable to a fine from BGN 500 to 1,000.

(2) Where an offence under paragraph 1 has been committed by a legal person in the course of its operations, such person shall be liable to pay damages from BGN 1,000 to 5,000.

Article 130

(1) Whoever commits or fails to prevent an offence under Article 108(3) shall be liable to a fine from BGN 500 to 2,000, unless the offence is a criminal one.

(2) Where an offence under paragraph 1 has been committed by a legal person in the course of its operations, such person shall be liable to pay damages from BGN 1,000 to 3,000.

Article 131

Any head of organisational unit who fails to disclose information to the competent authorities as requested under the conditions and procedure of this Act shall be liable to a fine of BGN 500.

Article 132

(1) (Previous text of Article 132, SG No. 71/2016) Where no other penalty is provided for an offence under this Act and the implementing statutory instruments hereto, the offender shall be liable to a fine from BGN 30 to 200.

(2) (New, SG No. 71/2016) For an offence under article 1 committed by a head of an organisational unit the fine shall be from BGN 200 to BGN 2000.

Article 133

Where an offence under Articles 117 - 132 is a repeated offence, the fine, or as the case may be, the damages imposed shall be equal to double the original amounts.

Article 134

(1) (Amended, SG No. 109/2007, supplemented, SG No. 36/2008) The statement establishing an offence under any of the foregoing Articles shall be drawn up by such official persons as the chairperson of SISC, or the Chairperson of the State Agency for National Security, shall authorise, and the relevant penal order shall be issued by the chairperson of SISC or, within his respective terms of reference, by the Chairperson of the State Agency for National Security, or by an appointed by him Deputy Chairperson.

(2) The offences hereunder shall be established, and the relevant penal orders shall be issued, appealed, and enforced, under the procedure laid down in the Administrative Violations and Sanctions Act.

SUPPLEMENTARY PROVISIONS

§ 1. Within the meaning of this Act:

1. (Amended, SG No. 109/2007, SG No. 69/2008, SG No. 93/2009, effective 25.12.2009, SG No. 52/2013, effective 14.06.2013, SG No. 70/2013, effective 9.08.2013, supplemented, SG No. 14/2015, amended, SG No. 79/2015, effective 1.11.2015, supplemented, SG No. 81/2016, effective 14.10.2016, amended, SG No. 7/2018, SG No. 69/2020, SG No. 84/2023, effective 6.10.2023) "Security services" are the State Intelligence Agency, the National Service for Protection, the State Agency for National Security, the Combat Against Organised Crime Directorate General and the Internal Security Directorate at the Ministry of Interior, the Military Intelligence Service at the Ministry of Defence, the State Agency for Technical Operations the Counter-Corruption Commission;

2. (Amended, SG No. 82/2006, supplemented, SG No. 109/2007, amended, SG No. 69/2008, SG No. 93/2009, effective 25.12.2009, SG No. 88/2010, effective 1.01.2011, SG No. 48/2011, effective 24.06.2011, SG No. 44/2012, effective 1.07.2012, SG No. 53/2014, SG No. 14/2015, SG No. 81/2016, effective 14.10.2016, supplemented, SG No. 60/2020, effective 1.10.2020) "Public order services" are the National Police Directorate General, General Directorate Gendarmerie, Special Operations and Anti-Terrorism, the Border Police Directorate General, the National Fire Safety and Protection of Population Directorate General, the regional directorates of the MoI and the Military Police Service with the Minister of Defence;

3. (Amended and supplemented, SG No. 35/2009, effective 12.05.2009, amended, SG No. 16/2010, effective 26.02.2010, SG No. 23/2011, effective 22.03.2011, supplemented, SG No. 62/2022) "Organisational unit" are: any government authority and its administration; the administration under Paragraph 10 of Article 136 of the Judicial System Act, the Ministry of

Defence and any units directly subordinate to the Minister of Defence and selected by the latter, including formations of the Bulgarian Army, any authority of local self-government and local administration, and any public-law entity created by law or by an instrument of the executive branch, and any natural or legal person which generates, processes, stores or releases classified information;

4. "Information security officer" is any natural person, such as appointed by the head of an organisational unit to perform the activities relating to the protection of classified information within such organisational unit;

5. (Supplemented, SG No. 36/2008) "Competent authority", for the purposes of issuance, termination, revocation, and denial of clearance for access to classified information, is SISC, the head of any security service or public order service, or their deputies if they are appointed by them, and any information security officer;

6. "Unauthorised access to classified information" is the divulgence, misuse, modification, damage, disclosure, destruction of classified information, and any other action compromising the protection, or resulting in the loss of such information. Unauthorised access shall be deemed to be also any omission to classify information by the appropriate marking, or the improper choice of classification marking, and any action or omission resulting in knowledge of such information being acquired by any person who does not possess the appropriate clearance or confirmation;

7. "Registry" is a separate structure which registers, receives, sends, distributes, prepares, reproduces, releases, and stores classified information;

8. "Registry in the field of international relations" is a registry created in pursuance of an international treaty to which the Republic of Bulgaria is a party;

9. "Security marking" is the marking on any material containing classified information which shows the classification level of such material;

10. "Material" is any document or any other object of technical nature, or facility or equipment or device or armament, whether finished or in process, and any component thereof used in the manufacture thereof;

11. "Document" is any recorded information, regardless of the physical form or characteristics thereof, including the following information media: any handwritten or typed material, any data processing software, any stamp, map, table, photograph, drawing, colouring, etching, technical drawing, or any part thereof, and any sketch, draft copy, preparatory notes, carbon copy, ink ribbon, and any form of reproduction by any device or process, such as sound, voice, magnetic recording, video recording, electronic recording, optical recording, and any portable equipment or device for electronic data processing on fixed or removable media, etc;

12. "Compilation of materials and/or documents" is any number of materials and/or documents brought together for any purpose under this Act, and relating to a single subject and arranged in certain order;

13. (Amended, SG No. 61/2015, effective 1.11.2015) "National security" is the concept referred to in Article 2 of the Act on the Management and Functioning of the System of National Security Protection;

14. "Interests of the Republic of Bulgaria as relate to national security" is the safeguarding of the sovereignty, the territorial integrity, and the constitutional order of the Republic of Bulgaria, including:

(a) the detection, prevention, and counteraction of any action detrimental to the country's independence and territorial integrity;

(b) the detection, prevention, and counteraction of any covert action posing a threat or causing a prejudice to the country's political, economic, and defence interests;

(c) the procurement of information about other countries or of foreign origin, such as is necessary for decisions to be made by the supreme authorities of the State and organs of governance;

(d) the detection, prevention, and counteraction of any covert action aimed at a violent change of the country's constitutional order, which guarantees the exercise of human and civil rights, and democratic representation on the basis of a multi-party system, and the functioning of the institutions established by the Constitution;

(e) the detection, prevention, and counteraction of any terrorist action, or the illegal trafficking in human beings, weapons, and drugs, and the illegal trafficking in products and technologies placed under international control, and money laundering, or any other specific risks and threats;

15. "Damage in the field of national Security, defence, foreign policy or the protection of the constitutional order" is any threat or prejudice to the interests of the Republic of Bulgaria, or to such interests as the Republic of Bulgaria has undertaken to safeguard, the harmful consequences of which are incapable of being eliminated or are only capable of being mitigated by subsequent measures. Depending on the importance of such interests, and on the gravity of such harmful consequences, the damage threatened or caused can be irreparable or exceptionally grave or nearly irreparable or grave or limited, where:

(a) irreparable or exceptionally grave damage is such as entails or might entail the complete or partial disruption of the national security or of the related interests of the Republic of Bulgaria as fundamental protected interests;

(b) nearly irreparable or grave damage is such as entails or might entail a significant negative impact on the national security or on the related interests of the Republic of Bulgaria as fundamental protected interests, which is incapable of being compensated without harmful consequences or without such harmful consequences as are only capable of being mitigated by considerable subsequent measures;

(c) limited damage is such as entails or might entail a negative impact of short duration on the national security or the related interests of the Republic of Bulgaria as fundamental protected interests, which is capable of being compensated without harmful consequences or with such harmful consequences as are capable of being mitigated by minor subsequent measures;

16. "Repeated" is such an offence under this Act or the implementing statutory instruments hereto as is committed within one year from the effective date of the penal order whereby a penalty was imposed for the same kind of offence;

17. "Systematic offences" are three or more offences under this Act or the implementing statutory instruments hereto committed within any one year;

18. "Generation, processing, storing, or release of classified information" is the generation, the marking, the registration, the storing, the use, the disclosure, the transformation, and the declassification of classified information;

19. (New, SG No. 88/2018) A "Communication and Information System (CIS)" shall mean a set of technical (including communications, border protection, cryptographic and broadcasting tools within the system) and software tools, methods, procedures and staff arranged to perform one or more of the functions related to the generation, processing, use, storage and exchange of classified information in electronic form. A communication and Information system may also be based on one or more isolated workstations not connected into a network.

20. (New, SG No. 88/2018) A "Closed-type information system" shall mean a system with protection measures in place without access to public networks, which is designed for handling non-classified information.

21. (New, SG No. 88/2018) "Interconnection" shall mean the connection between two or more CIS, or the connection of CIS to other information systems for the handling of non-classified information for the purpose of one-way or multiple-way exchange of data and other information resources. The connection between a CIS and a system providing only communication infrastructure for the transfer of classified information protected through cryptographic means which are approved in accordance with the procedure provided for in the regulation referred to in Article 85 shall not be regarded as interconnection.

22. (New, SG No. 88/2018) "CIS border" shall mean a physical or logical perimeter defining the boundaries of protection of the CIS concerned.

23. (New, SG No. 88/2018) A "Border protection mechanism" shall mean a set of components (software or technical tools) which are used for control, monitoring and filtering purposes in order to prevent unauthorised access to the classified information and the information resources in an interconnected CIS.

24. (New, SG No. 88/2018) "Compromising electromagnetic emanations" shall mean unintentionally emitted electromagnetic signals related to the operation of technical tools for the generation, processing, storage and transfer of classified information, which, if intercepted and analysed, may lead to unauthorised access to such classified information.

25. (New, SG No. 88/2018) "TEMPEST" shall mean the examination, study, and control of compromising electromagnetic emanations and the countermeasures to inhibit and curtail those.

26. (New, SG No. 88/2018) "TEMPEST countermeasures" shall mean security measures aiming to prevent unauthorised access to classified information through compromising electromagnetic emanations.

§ 2. Within the meaning of this Act, "official person" is any person under Article 93(1) of the Criminal Code.

§ 2a. (New, SG No. 42/2009, amended, SG No. 93/2009, effective 25.12.2009, SG No. 88/2010, effective 1.01.2011, supplemented, SG No. 44/2012, effective 1.07.2012, amended and supplemented, SG No. 52/2013, effective 14.06.2013, amended, SG No. 53/2014, SG No. 14/2015, SG No. 81/2016, effective 14.10.2016, SG No. 60/2020, effective 1.10.2020) For the purposes of Article 46, items 2 and 3 herein, the MoI Secretary General and Deputy Secretary General, the members of the political cabinet of the Minister of Interior and the expert and technical aides thereof, the Administrative Secretary of the Ministry of Interior, the officers and the candidate-officers of the Migration Directorate, of the International Operational Cooperation Directorate, of the directorates of the general and specialised administration, the administrative directorates, the Academy of the MoI, the Medical Institute, the MoI, the structures under Article 37, paragraph 4 of the Ministry of Interior Act, the cadets at the Ministry of Interior Academy, and the heads and the candidates for heads of the security and public order services in the Ministry of Interior shall be deemed employees of the Interior Security Directorate.

§ 2b. (New, SG No. 93/2009, effective 25.12.2009, amended, SG No. 88/2010, effective 1.01.2011, SG No. 44/2012, effective 1.07.2012, repealed, SG No. 52/2013, effective 14.06.2013).

TRANSITIONAL AND FINAL PROVISIONS

§ 3. Within three months from the entry into force of this Act, the Council of Ministers shall adopt the Detailed Rules for the Application hereof.

§ 4. Within three months from the entry into force of this Act, the Council of Ministers shall:

1. adopt the regulations under Articles 13, 78, 85, 90(1), and 95(2);

2. bring into consistency with this Act the Secret Patents Regulation (SG No. 81/1993), subject to the advice of the chairperson of the Patents Office.

§ 5. Within three months from the entry into force of this Act, the Minister of Health shall, in consultation with SISC, issue the regulation under Article 42(3).

§ 6. Within one month from the entry into force of this Act, the Council of Ministers shall create the State Information Security Commission and shall adopt its Institutional Rules.

§ 7. Within three months from the entry into force of this Act, the heads of organisational units shall appoint information security officers, excepting the circumstances under Article 20(3), and shall create administrative security units in pursuance of Article 23.

§ 8. Within three months from the entry into force of this Act, the heads of organisational units and the heads of the security services and the public order services shall draw up the lists under Article 37.

§ 9. (1) Any materials and documents prepared before the entry into force of this Act, and marked as "Top Secret of Special Importance", "Top Secret", or "Secret", shall be deemed to be marked respectively as "Top Secret", "Secret", and "Confidential", and the respective durations of classification shall be determined in pursuance of Article 34(1) and shall be deemed to have commenced with the date of preparation such material or document.

(2) Within one year from the entry into force of this Act, the heads of organisational units shall review and bring into consistency with this Act and the implementing statutory instruments hereto the materials and documents which contain classified information.

§ 10. (1) The access permits issued in pursuance of the provisions existing before the entry into force of this Act shall continue to be valid until the replacement thereof with clearances for access. The heads of organisational units, employing persons who possess an access permit and whose positions or special assignments require access to the classified information, shall request the issuance of clearances for access in accordance with the requirements of this Act and within three months from its entry into force. Non-compliance with this provision shall result in the invalidation of the existing access permits.

(2) The background investigation and clearance procedure for the purposes of paragraph 1 shall be completed within such time limit as SISC shall prescribe, but not exceeding 18 months.

§ 11. (Corrected, SG No. 5/2003) Any pending issuance procedure for an access permit to secret information shall be transformed into a background investigation procedure under this Act.

§ 11a. (New, SG No. 93/2009, effective 25.12.2009) Any investigation procedure and issuance procedure for an access permit to classified information which have commenced in respect of employees referred to in § 2a and 2b of the Supplementary Provisions shall be completed as per the existing practice.

§ 12. In Article 20(1), subparagraph 2, of the Cadastral Survey and Property Register Act (SG No. 32/2000), the words "protect as an official secret the data which came to his knowledge" are replaced with the words "protect the classified information, being an official secret, which came to his knowledge".

§ 13. Article 20 of the Constitutional Court Act (SG No. 67/1991, amended, SG No. 25/2001) is amended as follows;

1. In paragraph 2, the words "State or official secret" are replaced with the words "classified information which is a State secret or an official secret".

2. New paragraph 3 is inserted as follows:

"(3) In the circumstances under paragraph 2, the conditions and procedure laid down in the Protection of Classified Information Act shall apply."

§ 14. The Republic of Bulgaria Defence and Armed Forces Act (SG No. 112/1995, amended

and supplemented, SG No. 67/1996, SG No. 122/1997, SG No. 70, 93, 152 and 153/1998, SG No. 12, 67 and 69/1999, SG No. 49 and 64/2000, SG No. 25/2001, SG No. 1 and 40/2002 amended) is amended as follows:

1. In Article 5, the words "State or official secret" are replaced with the words "classified information which is the State or an official secret".

2. Article 32(9) is repealed.

3. In Article 35(1), subparagraph 14, the words "State or official secret" are replaced with the words "classified information which is a State secret or an official secret".

4. In Article 78(1), subparagraph 16, the words "State or official secret" are replaced with the words "classified information which is the State or an official secret".

5. In Article 200, the words "State or official secret" are replaced with the words "classified information".

6. In Article 273, the words "State or official secret" are replaced with the words "classified information".

7. In Article 281(1), the words "State or official secret" are replaced with the words "classified information which is the State or an official secret".

§ 15. In Article 9(2) of the Foreign Exchange Act (SG No. 83/1999), the words "and official secret" are replaced with the words "secret and the requirements relating to the protection of classified information which is an official secret".

§ 16. In Article 3 (3) of the Carriage by Road Act (SG No. 82/1999, amended, SG No. 11/2002), the word "official" are replaced with the words "classified information which is an official secret".

§ 17. In Article 15 (3) of the Administrative Procedure Act (SG No. 90/1979, amended, SG No. 9/1983, 26/1988, 94/1990, 25 and 61/1991, 19/1992, 65 and 70/1995, 122/1997, 15 and 89/1998, 83 and 95/1999), the words "protection of" are replaced with the words "protection of classified information which is".

§ 18. In § 5 of the Other Provisions of the Refugees Act (SG No. 53/1999, amended), the words "official secret" are replaced with the words "classified information which is an official secret".

§ 19. In Article 52 of the Banking Act (SG No. 52/1997, amended and supplemented, SG No. 15, 21, 52, 70 and 89/1998, 54, 103 and 114/1999, 24, 63, 84 and 92/2000, 1/2001), new paragraph 8 is inserted as follows:

"(8) The banks shall have a duty, at the written request of the chairperson of SISC or of the head of any security service or public order service, to provide information about the account balances and transactions of any person under a background investigation pursuant to the Protection of Classified Information Act. Such request shall be accompanied by such person's consent to the disclosure of such information."

§ 20. The Bulgarian Identity Documents Act (SG No. 93/1998, amended, SG No. 53, 67, 70 and 113/1999, 108/2000, 42/2001) is amended as follows:

1. In Article 75, new paragraph 2 is inserted as follows:

"2. persons about whom sufficient evidence exists that by such travel they might pose a threat to the system for the protection of classified information which is the State secret of the Republic of Bulgaria;"

2. In Article 78, the existing text is placed under paragraph 1 and new paragraph 2 is inserted as follows:

"(2) The involuntary administrative measure under Article 75(2) shall be taken in pursuance of a reasoned order of the chairperson of the State Information Security Commission

or of the head of any security service or public order service."

3. In Article 79(1) and (2), the reference "Article 75(1) and (3)" are replaced with the reference "Article 75 (1) - (3)".

§ 21. The Ministry of the Interior Act (SG No. 122/1997, Judgment No. 3/1998 of the Constitutional Court - SG No. 29/1998, amended, SG No. 70, 73 and 153/1998, 30 and 110/1999, 1 and 29/2000, 28/2001) is amended as follows:

1. In Article 7(14), the words "encryption operations within the Republic of Bulgaria and within its representations abroad" are replaced with the words "cryptographic protection of classified information within the Republic of Bulgaria and within its diplomatic and consular missions".

2. In Article 46(1), subparagraph 7, the words "protection of the facts, information, and objects which are a State secret" are replaced with the words "protection of classified information which is a State secret or an official secret".

3. Article 51(1) is amended as follows:

"(1) The National Security Service performs activities in connection with the functioning of the National System for the Protection of Classified Information which is a State Secret or an Official Secret in pursuance of the Protection of Classified Information Act."

4. In Article 52(1), the words "protection of the facts, information, and objects which are a State secret" are replaced with the words "protection of classified information".

5. Article 53 is repealed.

6. Article 124 is amended as follows:

"124. (1) The Communication Devices Protection Directorate is a special directorate of the Ministry of Home Affairs responsible for the cryptographic protection of classified information within the Republic of Bulgaria and within its diplomatic and consular missions, and for the acquisition, organisation and processing of information from foreign sources in the interest of national security, and for the operational control of the national radio frequency spectrum, by:

1. evaluation and development of cryptographic algorithms and devices for cryptographic protection of classified information; development and distribution of cryptographic keys; approval and control of the use, manufacture and import of cryptographic protection devices;

2. issuance of security certificates of automated information systems or networks used for classified information; coordination and control of the electromagnetic interference countermeasures protecting the technical devices used for the processing, the storing, or the transmission of classified information;

3. organisation and operation of the communications between the Republic of Bulgaria and its diplomatic and consular missions, and cryptographic protection of the information so exchanged by the provision of the necessary personnel for the departmental units and for the diplomatic and consular missions;

4. acquisition, processing, and organisation of information by technical devices from the technical sources of other States in the interest of national security, and release of such information to such users as shall be designated by an order of the Minister of Home Affairs or by law;

5. detection and prevention of any use of the national radio frequency spectrum against the country's security or contrary to the law, and joint actions with the competent government authorities;

6. provision and use of special surveillance devices, and preparation of investigation exhibits under such conditions and procedure as shall be provided by law;

7. operational searches;

8. joint actions with the other services of the Ministry of Home Affairs and with the special government authorities, and with the counterpart services of other States, within its terms of reference;

9. information activities.

(2) The relevant departments shall provide funding support to the units under paragraph 1, subparagraph 3, and such units within diplomatic or consular missions.

(3) The organisation of activities under paragraph 1, subparagraph 3, shall be provided for by a regulation of the Council of Ministers."

7. Article 162(3) is repealed.

8. In Article 187, the words "protection of the facts, information, and objects which are a State secret" are replaced with the words "protection of classified information".

§ 22. The Bulgarian National Bank Act (SG No. 46/1997, amended, SG No. 49 and 153/1998, 20 and 54/1999, 109/2001) is amended as follows:

1. In Article 4(2), after the words "credit relations", a comma is inserted and the words "excepting the circumstances under the Protection of Classified Information Act".

2. In Article 23(2), the words "which are an official" are replaced with the words "which is classified information, being an official".

§ 23. The Access to Public Information Act (SG No. 55/2000, amended, SG No. 1/2002) is amended as follows:

1. In Article 7(1), the word "is" is replaced with the words "is classified information, being".

2. In Article 9(2), the words "State or official secret" are replaced with the words "classified information which is a State or an official secret".

3. In Article 13(3), the words "20 years" are replaced with the words "two years".

4. In Article 37(1), subparagraph 1, the words "State or official secret" are replaced with the words "classified information which is a State or an official secret".

5. In Article 41(4), the word "classification" is replaced with the words "placement of security marking".

§ 24. The State Property Act (SG No. 44/1996, amended, SG No. 104/1996, 55, 61 and 117/1997, 93 and 124/1998, 67/1999, 9, 12, 26 and 57/2000, 1/2001; Judgment No. 7/2001 of the Constitutional Court - SG No. 38/2001) is amended as follows:

1. In Article 70(2), the words "State secret" are replaced with the words "classified information which is a State or an official secret".

2. In Article 78(2), the words "State secret" are replaced with the words "classified information which is a State or an official secret".

§ 25. Article 25 of the Civil Servants Act (SG No. 67/1999, amended, SG No. 1/2000, 25, 99 and 110/2001) is amended as follows:

"Protection of Classified Information Which Is a State or an Official Secret

25. (1) Every civil servant shall have a duty to protect the classified information, which is a State or an official secret, which came to his knowledge in the course of, or in connection with, the pursuance of his official duties.

(2) The classified information which is a State or an official secret, and procedure for operation therewith, shall be defined by law."

§ 26. Article 17 of the Act Restoring Ownership of Forests and Forest Stock Land Tracts (SG No. 110/1997, amended, SG No. 33, 59 and 133/1998, 49/1999, 26 and 36/2001) is amended as follows:

1. The existing text is placed under paragraph 1 and the words "including such as are a

State secret" are deleted.

2. New paragraph 2 is inserted as follows:

"(2) Where the information under paragraph 1 is classified information, the release thereof shall be governed by the Protection of Classified Information Act."

§ 27. In Article 11(1) of the Postal Services Act (SG No. 64/2000, amended, SG No. 112/2001), the words "secret correspondence" are replaced with the words "correspondence which contains classified information".

§ 28. Article 9 of Decree No. 612, Chapter 2, on Seals and Stamps (SG No. 69/1965, amended, SG No. 26/1988, 11 and 47/1998) is repealed.

§ 29. In Article 6 (1) of the Public Procurement Act (SG No. 56/1999, amended, SG No. 92 and 97/2000, 43/2002), the words "are the subject of a State secret" are replaced with the words "are the subject of classified information which is a State secret".

§ 30. The Statistics Act (SG No. 57/1999, amended, SG No. 42/2001) is amended as follows:

1. In Article 22, the words "protection of secrets" are replaced with the words "protection of classified information".

2. Article 27(2) is amended as follows:

"(2) The registration, the use, the processing, and the storing of statistical data which are classified information shall be governed by the provisions of the legislative and the statutory instruments relating to the protection of classified information."

§ 31. The National Audit Office Act (SG No. 109/2001) is amended as follows:

1. In Article 30 (1), the words "State, official" are replaced with the words "classified information which is a State or an official secret, and".

2. In Article 31, new paragraph 7 is inserted as follows:

"(7) Where the exercise of the powers under paragraph 1 requires access to classified information, the relevant conditions and procedure laid down in the Protection of Classified Information Act shall apply."

§ 32. Article 6 (2), second sentence, of the Act to Transform the Construction Corps, the Transport Ministry Troops and the Posts and Telecommunications Committee Troops into State-Owned Enterprises (SG No. 57/2000) is amended as follows:

"They can perform and award public procurement contracts relating to the country's defence or security and having as their subject matter classified information which is a State secret, and the performance thereof shall be governed by the provisions of the Protection of Classified Information Act."

§ 33. Article 32(2) of the Social Assistance Act (SG No. 56/1998) is amended as follows:

"(2) The inspectors shall have a duty to comply with the provisions of the legislative and the statutory instruments relating to the protection of classified information with regard to such information as came to their knowledge in the course of, or in connection with, an inspection, and shall have a duty to respect the honour and the dignity of the assistance beneficiaries."

§ 34. The Patents Act (SG No. 27/1993, amended, SG No. 11/1998, 81/1999) is amended as follows:

1. Article 24 is amended as follows:

"24. (1) Secret patents shall be issued with respect to inventions which contain classified information which is a State secret within the meaning of Article 25 of the Protection of Classified Information Act.

(2) At the filing of a secret patent statement, the applicant shall have a duty to state that the subject invention is a matter of State secret.

(3) The level at which the invention under paragraph 2 shall be classified shall be determined by the appropriate competent authority, to the activities of which the invention relates, subject to consultation with the State Information Security Commission.

(4) The competent authority under paragraph 3 shall decide within three months from the date of referral and shall advise the Patents Office accordingly. The secret patent statement shall be identified with the appropriate security marking, in accordance with the competent authority's decision, and the applicant shall be advised accordingly.

(5) If, within the time limit under paragraph 4, the Patents Office is not advised of classification level, the subject statement shall be deemed to be free of any information which is a State secret. The Patents Office shall advise the applicant that the subject invention does not contain any classified information which is a State secret and shall require the applicant's express consent to the review of his statement under the general procedure. If the applicant fails to give such consent, the statement shall be deemed to have been withdrawn and the relevant material shall be returned to the applicant.

(6) Where the competent authority under paragraph 3 is an applicant and where, subject to consultation with the State Information Security Commission, the statement has been security-marked in accordance with the classification level of the invention, the procedure under paragraphs 4 and 5 shall not apply.

(7) The Patents Office shall only publish the numbers of secret patents issued, at no charge."

2. Article 25(2) is amended as follows:

"(2) The competent authorities under Article 24(3) may, subject to consultation with the State Information Security Commission, ban the patenting abroad of any invention which contains classified information which is a State secret."

3. In Article 31(5), the words "subject to the prior written consent of the Ministry of Defence or the Ministry of Home Affairs" are replaced with the words "under the conditions and procedure laid down in the Protection of Classified Information Act".

4. In Article 32(8), the words "only by the Council of Ministers, at the request of the Ministry of Defence or of the Ministry of Home Affairs" are replaced with the words "by the State Information Security Commission".

5. In Article 45(3), the words "the Ministry of Defence or of the Ministry of Home Affairs" are replaced with the words "the competent authorities under Article 24(3), subject to consultation with the State Information Security Commission".

6. Article 46(3) is repealed.

7. In Article 48, the reference "Article 46(1), (2), and (3)" is replaced with the reference "Article 46(1) and (2)".

8. Article 50 is amended as follows:

(a) paragraph 1, subparagraph 3, is amended as follows:

"3. the statement is made for the issuance of a secret patent for an invention which contains classified information which is a State secret;"

(b) paragraph 3 is amended as follows:

"(3) The Patents Office shall publish where, pursuant to Article 34 of the Protection of Classified Information Act, no legal reasons exist any longer for the classification of information contained in the invention as a State secret."

9. In Article 55(1), subparagraph 1, the reference "Article 46(2) and (3)" is replaced with the reference "Article 46(2)".

10. Article 67(6) is amended as follows:

"(6) Where the Republic of Bulgaria designates itself in pursuance of Article 8(2), subparagraph (b), of the Treaty, the Patents Office shall refer the international statement to the competent authorities, to the activities of which such invention relates, for the determination of a classification level. Such determination shall be governed by the provisions laid down in the Protection of Classified Information Act and shall be completed within the time limit under Article 24(4) of the same. If it is established that such international statement contains information classified as a State secret, it shall not be treated as an international statement and shall not be distributed officially and shall not be published."

11. In Article 84(1), the words "secret statement" are replaced with the words "secret patent statement", and the words "from BGN 100 to 1,000" are replaced with the words "from BGN 1,000 to 20,000".

§ 35. In Article 99 (1) of the Telecommunications Act (SG No. 93/1998, amended, SG No. 26/1999, 10 and 64/2000, 34, 42, 96 and 112/2001), the words "national encryption authority" are replaced with the words "Communication Devices Protection Directorate".

§ 36. In Article 33 (2) of the Local Self-government and Local Administration Act (SG No. 77/1991, amended, SG No. 24, 49 and 65/1995, 90/1996, 122/1997, 33, 130 and 154/1998, 67 and 69/1999, 26 and 85/2000, 1/2001, 28/2002), the words "State or official secret within the meaning of the law" are replaced with the words "classified information which is a State or an official secret".

§ 37. (1) The Access to the Documents Act of the Former State Security Police and the Former Intelligence Service of the General Staff (SG No. 63/1997, as Judgment No. 10/1997 of the Constitutional Court - SG No. 89/1997, amended, SG No. 69/1999, 24/2001; Judgment No. 14/2001 of the Constitutional Court - SG No. 52/2001; amended, SG No. 28/2002) is repealed.

(2) The appropriations under the National Budget Act for 2002 to, and the fixed tangible assets of, the government authorities under the Access to the Documents Act of the Former State Security Police and the Former Intelligence Service of the General Staff, which have ceased to exist, shall be transferred to the State Information Security Commission.

§ 38. Articles 284a and 313b of the Criminal Code (SG No. 26/1968, corrected, SG No. 29/1968, amended and supplemented, SG No. 92/1969, 26 and 27/1973, 89/1974, 95/1975, 3/1977, 54/1978, 89/1979, 28/1982; corrected, SG No. 31/1982; amended and supplemented, SG No. 44/1984, 41 and 79/1985; corrected, SG No. 80/1985; amended and supplemented, SG No. 89/1986; corrected, SG No. 90/1986; amended, SG No. 37, 91 and 99/1989, 10, 31 and 81/1990, 1, 86, 90 and 105/1991, 54/1992, 10/1993, 50/1995; Judgment No. 19/1995 of the Constitutional Court - SG No. 97/1995; amended, SG No. 102/1995, 107/1996, 62 and 85/1997; Judgment No. 19/1997 of the Constitutional Court - SG No. 120/1997; amended, SG No. 83, 85, 132, 133 and 153/1998, 7, 51 and 81/1999, 21 and 51/2000; Judgment No. 14/2000 of the Constitutional Court - SG No. 98/2000; amended, SG No. 41/2001, 101/2001) are repealed.

§ 39. Article 24 (1), subparagraphs 9 and 10, Article 29 (2), Article 48 (5), and § 6 of the Transitional and Final Provisions, of the Election of Members of Parliament Act (SG No. 37/2001, Judgment No. 8/2001 of the Constitutional Court - SG No. 44/2001) are repealed.

§ 40. Article 42a of the Election of Grand National Assembly Act (SG No. 28/1990, amended, SG No. 24/2001) is repealed.

§ 41. Article 8 (2) of the Election of President and Vice President of the Republic Act (SG No. 82/1991, amended, SG No. 98/1991, 44/1996, 59/1998, 24, 80 and 90/2001) is repealed.

§ 42. Article 42 (4) of the Local Elections Act (SG No. 66/1995, corrected, SG No. 68/1995; Judgment No. 15/1995 of the Constitutional Court - SG No. 85/1995; amended, SG No. 33/1996; Judgment No. 4/1998 of the Constitutional Court - SG No. 22/1998; amended, SG No. 11 and

59/1998, 69 and 85/1999, 29/2000, 24/2001) is repealed.

§ 43. The List of Facts, Data and Objects Which Are a State Secret of the Republic of Bulgaria (SG No. 31/1990, amended, SG No. 90 and 99/1992, 108/1999, 55/2000) is repealed.

TRANSITIONAL PROVISION

to the Act for Amendment and Supplement the Classified
Information Protection Act
(Promulgated, State Gazette No. 95/2007)

§ 10. (1) The protection period of the materials and documents prepared before the entry into force of this Act, and marked as "For Official Use Only", shall be calculated in accordance with Article 34, paragraph 1 and shall be counted as of the date when they were created.

(2) Within 6 months after the entry into force of this Act, the heads of the organizational units shall review the materials and documents classified as official secret and bring them into consistency with the requirements of the Act.

TRANSITIONAL AND FINAL PROVISIONS

to the Act Amending and Supplementing the Administration Act
(SG No. 42/2009)

§ 47. Paragraph 2a of the Supplementary Provisions of the Classified Information Protection Act shall not apply in respect of employees, as specified therein, who were subject to procedures, commenced prior to the entry into force of this Act, for screening and issuance of a permit allowing access to classified information.

.....
TRANSITIONAL AND FINAL PROVISIONS to the Act Amending and
Supplementing the Republic of Bulgaria Defence and Armed Forces Act
(SG No. 16/2010, effective 26.02.2010)

.....
§ 149. The Classified Information Protection Act (promulgated, SG No. 45/2002; amended, SG No. 5/2003; amended, SG No. 31/2003, SG No. 52, 55 and 89/2004, SG No. 17 and 82/2006, SG No. 46, 57, 95 and 109/2007, SG No. 36, 66, 69 and 109/2008 and SG No. 35, 42, 82 and 93/2009) is amended as follows:

.....
3. The words "the structures of the Ministry of Defence" shall be replaced by "the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army".

.....
TRANSITIONAL AND FINAL PROVISIONS

to the Act Amending and Supplementing the Ministry of Interior Act
(SG No. 88/2010, effective 9.11.2010)

.....
§ 97. The following amendments and supplements shall be made to the Classified Information Protection Act (promulgated, SG No. 45/2002, corrected, SG No. 5/2003, amended, SG No. 31/2003, supplemented, SG No. 52/2004, No. 55/2004, SG No. 89/2004, amended, SG No. 17/2006, amended, SG No. 82/2006, SG No. 46/2007, SG No. 57/2007, amended and supplemented, SG No. 95/2007, SG No. 109/2007, SG No. 36/2008, supplemented, SG No. 66/2008, amended, SG No. 69/2008, supplemented, SG No. 109/2008, amended and supplemented, SG No. 35/2009, supplemented, SG No. 42/2009, amended, SG No. 82/2009,

amended and supplemented, SG No. 93/2009, amended, SG No. 16/2010):

.....
§ 117. The Act shall become effective from the day of its promulgation in the State Gazette, except § 1 - 23, § 25, § 27 - 30, § 32 - 34, § 40, § 41, § 43 - 55, § 63 - 89 and § 91 - 114, which shall become effective from 1.01.2011.

.....
FINAL PROVISIONS to the Addition
the Protection of Classified Information
(SG No. 103/2012)

§ 3. Within two months of the entry into force of this Act the Council of Ministers shall adopt the necessary amendments to the ordinance under Article 90, Paragraph 1.

TRANSITIONAL AND FINAL PROVISIONS
to the Act Amending and Supplementing
the Classified Information Protection Act
(SG No. 71/2016)

§ 18. (1) Within one year of the entry into force of this Act the background investigation authority, with the exception of the State Intelligence Agency and the Military Information Service of the Ministry of Defence shall address a written request under Article 27 of the Access to and Disclosure of the Documents and Announcing the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian Popular Army Act for the officials with access to classified information for whom no background investigation has not been conducted. The Commission for Disclosure of Documents and Announcement of the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian People's Army shall inform of its results, within three days after the conclusion of the investigation, the investigation authority, and in case of establishing affiliation - also the SISC and the investigated person.

(2) In case of a lack of written consent under Article 27, paragraph 2 of the Access to and Disclosure of the Documents and Announcing the Affiliation of Bulgarian Citizens with the State Security Service and the Intelligence Services of the Bulgarian Popular Army Act the validity of the clearance for access to classified information of the person under paragraph 1 shall be terminated.

§ 19. In case of established affiliation of a person under the preceding paragraph to State Security of the intelligence services of the Bulgarian People's Army an assessment of reliability shall be performed pursuant to Article 40, paragraph 1, items 6 and 8 under the procedure of Chapter Five.

§ 20. The existing proceedings on appeals against denials to issue clearance for access to classified information or against revoking clearances for access to classified information issued on the grounds of Article 40, paragraph 1, item 5 shall be concluded under the procedure herein.

§ 21. The denials for issuing clearances, which have entered into force, for access to classified information or revocations of clearances for access to classified information issued on the grounds of Article 40, paragraph 1, item 5, for which the terms under Article 57, paragraph 6 and Article 59, paragraph 6 have not expired, shall be revoked.

.....
TRANSITIONAL AND FINAL PROVISIONS
to the Act for Amendment and Supplement
the Classified Ministry of Interior Act
(SG No. 81/2016, effective 1.01.2017)

.....
§ 102. This Act shall enter into force on 1 January 2017 with the exception of:

1. paragraphs 6 – 8, § 12, item 1, 2 and 4, § 13, § 14, § 18 – 20, § 23, § 26 – 31, § 32, item 1 и 4, § 33 – 39, § 41 – 48, § 49 relating to Article 187, paragraph 3, first sentence, § 50 – 59, § 61 – 65, § 81 – 85, § 86, items 4 and 5, § 87, item 3, § 90, item 1, § 91, item 2 and 3, § 92, § 93 and § 97 – 101, which shall enter into force on the day of the promulgation of the Act in the State Gazette;

2. paragraph 32, items 2 and 3, § 49 relating to Article 187, paragraph 3, new second sentence, § 69 – 72, § 76 relating to the persons under § 70, § 78 in relation to the employees under § 69 and § 70, § 79 in relation to the employees under § 69 and § 70, § 91, item 1 and § 94, which shall enter into force on 1 February 2017.

TRANSITIONAL AND FINAL PROVISIONS

to the Act to Amend and Supplement the
Classified Information Protection Act
(SG No. 88/2018)

§ 17. (1) The acts on the implementation of this Act shall be issued or brought into compliance with this Act within six months after its entry into force.

(2) Any statutory instruments of secondary legislation issued prior to the adoption of the acts under Paragraph 1 shall continue to apply, insofar as they do not contradict this Act.

.....

FINAL PROVISIONS

to the Act to Amend and Supplement
the Military Intelligence Act
(SG No. 69/2020)

.....
§ 32. In the Classified Information Protection Act (promulgated, SG No. 45/2002, corrected, No. 5/2003, SG No. 31/2003, Nos. 52, 55 and 89/2004, Nos. 17 and 82/2006, Nos. 46, 57, 95 and 109/2007, Nos. 36, 66, 69 and 109/2008, Nos. 35, 42, 82 and 93/2009, Nos. 16 and 88/2010, Nos. 23, 48 and 80/2011, Nos. 44 and 103/2012, Nos. 52 and 70/2013, Nos. 49 and 53/2014, Nos. 14, 61, 79/2015, No. 28/2016, Decision No. 7 of the Constitutional Court of 2016 - No. 49/2016, Nos. 62, 71 and 81/2016, Nos. 97 and 103/2017, Nos. 7, 17, 44, 77 and 88/2018, No. 17/2019, No. 60/2020) everywhere in the text the words "Military Information" service" shall be replaced by "Military Intelligence Service".
.....

Schedule No.

1

to Article 25
(Supplemented, SG No. 52/2004,
SG No. 66/2008, effective 26.09.2008,
amended, SG No. 82/2009,
SG No. 93/2009, effective 25.12.2009,
SG No. 48/2011, effective 24.06.2011,
supplemented, SG No. 80/2011,
effective

14.10.2011,

amended, SG No. 70/2013,
effective

9.08.2013,

SG No. 49/2014,
amended and supplemented, SG No. 53/2014,
supplemented, SG No. 14/2015,
SG No. 79/2015, effective 1.11.2015,
SG No. 81/2016, effective 14.10.2016,
amended and supplemented, SG No. 44/2018,
amended, SG No. 88/2018,
SG No. 60/2020, effective 1.10.2020,
SG No. 80/2021)

Categories of Information to be Classified as a State Secret Listed

I. Information Relating to the Country's Defence

1. Structure, organisation, and functioning of the government authorities and of the Supreme Chief Command of the Armed Forces of the Republic of Bulgaria during a state of war, martial law or any other state of emergency.
2. Location, equipment, maintenance, operation, and security arrangements of the control centres of the central and the regional administration of the executive branch, and of the Armed Forces of the Republic of Bulgaria intended for use during a state of war, martial law or any other state of emergency.
3. Organisation and functioning of the communication and information systems of the authorities of the State and of the Armed Forces of the Republic of Bulgaria during the various states of defence alert or a state of war.
4. Information relating to the announcement of a higher state of nationwidedefence alert, war-time plans and estimates, projects and measures relatingto the nationwide defence readiness of the central and the regional administration of the executive branch, and of the manufacturers of military products. Information relating to the planning, the organisation, and functioning of the mobilisation deployment of the Armed Forces of the Republic of Bulgaria.
5. (Amended, SG No. 49/2014) Detailed structure of the armed forces, and information relating to the redeployment, the actual names, the organisation, the staff capacity and payroll, the armament and the control systems of the Armed Forces of the Republic of Bulgaria, or of any force, service or taskforce, group, detachment, special unit or facility, not included in the official exchange of data pursuant to the country's international commitments
6. Information relating to the tasks and the combat capabilities of the Armed Forces of the Republic of Bulgaria or of any force, service or taskforce, or of any potential enemy, and the likely areas or direction of hostilities.
7. Organisation, functioning and technical capabilities for the purposes ofelectronic intelligence gathering.
8. Organisation and functioning of the system for the bringing of the armedforces, of the central and the regional administration of the executive branch, and of the responsible legal persons to higher states of defence alert.
9. Strategic and operational documents presenting the warfare and operations concepts adopted by the armed forces.

10. Information relating to external threats of military nature to the State's security, and defence plans, analyses, and forecasts, and the decisions and tasks based thereon.
11. Information relating to the design, testing, manufacture, and placement into service of new prototype armaments, combat technologies, and munitions, and their respective mobilisation manufacturing capacities.
12. Information relating to the preparation of, and support for, the general national war-time plan, including the relevant physical, financial, and labour resources, and the instruments regulating this activity.
13. Organisation, deployment, armament, tasks, and capabilities of the intelligence units and organs.
14. Information relating to the defence- and security-related communication system and allocation of radio frequencies of the Republic of Bulgaria.
15. Plans and reports of allocations and spending in connection with concrete defence-related missions and tasks, as prescribed by the Council Ministers.
16. Plans, information, and aggregate data relating to the operational state of readiness within the national territory, and the construction of new war-time facilities.
17. Aggregate information relating to the special production of the defence industry, and development projections, plans, manufacturing capacities, research and development units for the performance of contracts for the supply of armaments, combat technologies, munitions, and military instrumentation.
18. (Supplemented, SG No. 52/2004, amended, SG No. 49/2014) Geodetic and cartographic materials and data, digital models and data, raster images, aerial films and photographs, photographic documents, which contain information about the type, the character, the purpose or the engineering equipment of facilities and areas of importance for the country's defence and security.
19. Tasks of the central and regional administration of the executive branch, and of the responsible legal persons, in a state of war or martial law or another state of emergency.
20. Organisation, functioning and management of the procurement system of the Armed Forces of the Republic of Bulgaria during a state of war, martial law or another state of emergency.
21. Data concerning the strategic stockpiles of war-time material resources.
22. Aggregate information relating to the imports and exports of armaments, combat technologies, and munitions for the purposes of the Armed Forces of the Republic of Bulgaria.
23. Planning, implementation, and results of research and development of particular importance for the defence and security of the Republic of Bulgaria.
24. Aggregate information relating to the relief and character (structure) of the sea and river beds. Elements which condition in real time the

hydrological status of littoral waters (excepting the watercourses listed for the purposes of international navigation). Data concerning established river crossings for the forces within the Republic of Bulgaria.

II. Information Relating to The Country's Foreign Policy and Domestic Security

1. Foreign policy information the unauthorised access to which might pose a serious threat to national security or might damage, or threaten grave damage to, the country's positions in negotiations with another State.
2. Information and documents relating to the domestic political and military situation in other States based on unpublished data the disclosure of which might threaten the country's national security.
3. Information relating to the organisation, the techniques and devices of special tasks implemented by operational searches and operational intelligence gathering by the security services or the public order services, and data concerning the special facilities of these services, and the information and objects obtained by such activities, and data making it possible to establish the identity of any person who has been or is of assistance in such activities.
4. (Amended, SG No. 93/2009, effective 25.12.2009, SG No. 48/2011, effective 24.06.2011, supplemented, SG No. 14/2015, SG No. 81/2016, effective 14.10.2016) Detailed organisational and staffing structure of the security services and the Military Police Service with the Minister of Defence, as well as aggregate data concerning the personnel thereof, except for the aggregate data regarding the officers of the Combat Against Organised Crime Directorate General and the Internal Security Directorate of the Ministry of Interior.
5. (Supplemented, SG No. 66/2008, effective 26.09.2008, SG No. 79/2015, effective 1.11.2015, amended, SG No. 44/2018) Identity data, or data which may make it possible to establish the identity, of persons who are not officers of the security services or the public order services but have provided or are providing cooperation to such services. Identifying data or data that may enable the identification of officers of the State Intelligence Agency performing operational and intelligence work.
6. Information relating to the use, pursuant to the relevant legal provisions, of special intelligence gathering devices (technical means and/or the techniques for their utilisation).
7. (Amended and supplemented, SG No. 53/2014, SG No. 44/2018, SG No. 60/2020, effective 1.10.2020, SG No. 80/2021) Data concerning the types, the availability, and the characteristics of the special equipment, armament, munitions, personal protection devices, instrumentation, and materials used by the security services, the public order services and the Protection Bureau with the Minister of Justice.
8. (Repealed, SG No. 70/2013, effective 9.08.2013).
9. Reports, statements, information bulletins, statistics, and other

data concerning the operations of the security services and the public order services.

9a. (New, SG No. 53/2014, amended, SG No. 60/2020, effective 1.10.2020)

An organisational and staff structure of the General Directorate "Gendarmerie, special operations and Anti-Terrorism" in relation to the structure in the general directorate conducting special operations and anti-terrorism operations, plans, reports, accounts and other documents containing information related to implementing the activity of this structure, as well as information on the identity of its servants when exercising their powers under Article 89, paragraph 1 of the Ministry of Interior Act.

9b. (New, SG No. 44/2018, amended, SG No. 80/2021) A detailed organisational and staff structure of the Protection Bureau with the Minister of Justice, information on the identity of the employees providing or implementing the special protection measures or the activities referred to in Article 14(3) of the Protection of Individuals at Risk in Relation to Criminal Proceedings Act, information on the organisation or implementation of special protection, identifying data or data that may enable the identification of individuals at risk or protected persons within the meaning of the same Act.

10. Information relating to budget allocations and spending, and government assets appropriated, to national security purposes.

11. Single registers of clearances, certificates, confirmations, or denial of access to classified information, and background investigation files maintained and kept by SISC.

12. Information relating to the manufacture and safe-keeping of stamps bearing the national coat of arms, and the stamps of the authorities of the State.

13. Classified information exchanged by the Republic of Bulgaria with international organisations or States and identified as "Top Secret", "Secret", "Confidential", or by any other equivalent marking.

14. (Amended, SG No. 88/2018) Information relating to the organisational, technical and software security of central and local government authorities' communication and information systems and other information processing systems.

15. Information relating to the design, implementation, procurement, and functioning of telecommunications, teleinformation, and postal networks used for the transfer of classified information which is a State secret for the purposes of the armed forces, the security services, or the support organisations of such systems or networks.

16. Passwords and access codes to devices which generate, process, store, and transmit information classified as "Top Secret", "Secret", "Confidential".

17. Organisation, methods, and devices for cryptographic protection of information classified as "Top Secret", "Secret", "Confidential"; descriptions or prototypes of devices under development or in operation for the protection of information so classified; key materials and classified information protected by cryptographic methods or devices.

18. Information relating to the transition of the economy from peace-

time to war-time state for the purposes of the various states of defence alert and during a state of war.

19. Information relating to the preparation, the organisation, and the operation of railway, road, and water transport facilities for the purposes of higher states of defence alert, nationwide or within the Armed Forces of the Republic of Bulgaria.

20. Information relating to the organisation, methods and devices for the protection of classified information which is a State secret.

21. (Amended, SG No. 49/2014) Information relating to the purpose, planning, and purchasing arrangements of special facilities, and their respective defence and security plans.

22. Information relating to persons suspected of any subversive, terrorist, or any other unlawful activity directed against the State's public order, security, defence, independence, integrity, or international status, as is gathered, verified or analysed by the security services or the public order services.

23. The system of forms and methods, and the operational capabilities of the national border guard, and the operations of the border checkpoints, and information relating to antiterrorist or antisabotage operations along the national border.

24. Aggregate data concerning the functioning of the system for the protection of classified information which is a State secret.

25. Electronic registers and journals for book-keeping purposes, and lists of any other materials, which contain classified information which is a State secret.

26. Materials of the Council of Ministers relating to the State's strategic potential and strategic government procurement for the purposes of national security.

27. (Amended, SG No. 82/2009) Information relating to the manufacturing technology and to the individual protection techniques employed for Bulgarian personal documents, banknotes, or other securities or legal tenders, or other documents with counterfeit protection, as issued by the authorities of the State or their administrations.

28. Information relating to foreign policy plans and tasks the disclosure of which might prejudice important interests of the State, prior to the official publication of such information.

29. Materials, documents, memorandums relating to international negotiations or consultations, and international treaties or parts thereof, if classified.

30. Organisation and functioning of diplomatic communications.

31. Security system of the Bulgarian diplomatic and consular missions.

32. War-time tasks of the Bulgarian diplomatic and consular missions.

33. War-time security arrangements for the diplomatic and consular missions, and the representations of international organisations, to the Republic of Bulgaria.

34. (New, SG No. 80/2011, effective 14.10.2011) Information and plans

under Articles 18a - 18e of the Disaster Relief Act.

III. Information Relating to the Country's Economic Security

1. Documents relating to negotiations on financing agreements of nationwide importance the disclosure of which might pose a threat to national security.
2. Research work commissioned by a government authority of particular importance for the interests of the national economy.
3. Information relating to technical, technological, or organisational solutions the disclosure of which might threaten to prejudice important economic interests of the State.
4. Information relating to the mode of operation of control and signalling devices, alarm systems, or security arrangements the disclosure of which might pose a threat to national security.
5. Political, economic, or military information concerning other States and provided to the Republic of Bulgaria under the condition that it shall be protected as classified.
6. Plans, projections, or information relating to the trade turnover of special equipment, special technologies or services with other States.
7. Information relating to inventions or utility models affecting the country's security or defence, as established in pursuance of the Patents Act.

Schedule No. 2
to Articles 47 and 48
(Amended and supplemented, SG No. 71/2016)

[Empty rectangular box for registration number and stamp]

(registration number and stamp of the organisational unit requesting background investigation for the purposes of access the classified information)

CONFIDENTIAL

(upon completion)

Photo 4/3,5

PERSONAL BACKGROUND INVESTIGATION
QUESTIONNAIRE
FOR THE PURPOSES OF ACCESS TO INFORMATION
CLASSIFIED AS A STATE SECRET

Pursuant to Articles 47 and 48 of the Protection Classified Information Act

This Questionnaire is to be used pursuant to the Act
for the purposes of your background investigation for access to information
classified as a State secret and properly identified

CONFIDENTIAL

SECRET

TOP SECRET

(please encircle as applicable)

I. PERSON'S UNDER INVESTIGATION PERSONAL DATA		
Name		
First name, father's name, family name		
Former names		
If applicable		

Date of birth									
---------------	--	--	--	--	--	--	--	--	--

Place of birth

State		Municipality	
Region		Inhabited place	
Citizenship			
Former citizenship			

Where citizenship has been changed,

--

Person in whose name the change or loss of foreign citizenship certificate was issued, or in whose name the current citizenship certificate was issued

Docum ent	No	issued on date								by				
Personal ID number														
Military rank														

Military passbook

Series				No	issued on date					by				
--------	--	--	--	----	----------------	--	--	--	--	----	--	--	--	--

Permanent domicile

State						Street							
Region						Neighbourhood, Block #							
Town (village)						Entrance, Apt. #							
ZIP code						Telephone							

Current domicile

State						Street				
Region					Neighbourhood, Block #					
Town (village)						Entrance, Apt. #				
ZIP code						Telephone				
ID Card	No		issued on date						by	

Place of work

--

name of company

BULSTAT No										
------------	--	--	--	--	--	--	--	--	--	--

Registered office

State		Street	
Town (village)		Office telephone	
ZIP code		Office fax	
Current position			
Latest monthly income		Currency	

Other place of work

--

name of company

BULSTAT No										
------------	--	--	--	--	--	--	--	--	--	--

Registered office

State		Street	
Town (village)		Office telephone	

ZIP code						Office fax	
Current position							
Latest monthly income						Currency	

Additional income sources for the latest full calendar year above BGN 5,000

Such as: leases, dividends, interest, stock market gains, income from investment funds, royalties, gambling proceeds exceeding the average monthly wages for the Republic of Bulgaria, corporate board member salaries, payments under procurement contracts, etc.

II. PERSON'S UNDER INVESTIGATION FATHER

Name	
------	--

First name, father's name, family name

Date of birth

Place of birth

State

Municipality

Region

Inhabited place

Citizenship

Permanent domicile

State

Street

Region

Neighbourhood, Block #

Town (village)

Entrance, Apt. #

ZIP code

Telephone

ZIP code						Office fax	
----------	--	--	--	--	--	------------	--

Current position	
------------------	--

III. PERSON'S UNDER INVESTIGATION MOTHER

Name	
------	--

First name, father's name, family name
--

Date of birth																			
---------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Place of birth	
----------------	--

State		Municipality	
-------	--	--------------	--

Region		Inhabited place	
--------	--	-----------------	--

Citizenship	
-------------	--

--	--	--	--

Permanent domicile

State		Street	
-------	--	--------	--

Region		Neighbourhood, Block #	
--------	--	------------------------	--

Town (village)		Entrance, Apt. #	
----------------	--	------------------	--

ZIP code						Telephone	

Current domicile

State		Street	
Region		Neighbourhood, Block #	
Town (village)		Entrance, Apt. #	
ZIP code		Telephone	
ID Card	No	issued on date	by

Place of work

--

name of company

BULSTAT No									
------------	--	--	--	--	--	--	--	--	--

Registered office

State		Street	
Town (village)		Office telephone	

ZIP code						Office fax	
Current position							
IV. PERSON'S UNDER INVESTIGATION SIBLINGS							
Name							
First name, father's name, family name							
Date of birth							

Place of birth

State		Municipality	
Region		Inhabited place	
Citizenship			

Permanent domicile

State		Street	
Region		Neighbourhood, Block #	

Town (village)		Entrance, Apt. #	
ZIP code		Telephone	

Current domicile

State		Street	
Region		Neighbourhood, Block #	
Town (village)		Entrance, Apt. #	
ZIP code		Telephone	
ID Card	No	issued on date	y b

Place of work

--

name of company

BULSTAT No									
------------	--	--	--	--	--	--	--	--	--

Registered office

State		Street	
-------	--	--------	--

Town (village)										Office telephone	
ZIP code										Office fax	
Current position											

V. PERSON'S UNDER INVESTIGATION SPOUSE OR COHABITANT

Name											
First name, father's name, family name											
Date of birth											

Place of birth

State		Municipality	
Region		Inhabited place	
Citizenship			

Permanent domicile

State		Street	
-------	--	--------	--

Region		Neighbourhood, Block #	
Town (village)		Entrance, Apt. #	
ZIP code		Telephone	

Current domicile

State		Street	
Region		Neighbourhood, Block #	
Town (village)		Entrance, Apt. #	
ZIP code		Telephone	
ID Card	No	issued on date	y b

Place of work

--

name of company

BULSTAT No									
------------	--	--	--	--	--	--	--	--	--

Registered office

State						Street		
Town (village)						Office telephone		
ZIP code						Office fax		
Current position								
VI. PERSON'S UNDER INVESTIGATION CHILDREN ABOVE THE AGE OF 14								
Name								
First name, father's name, family name								
Date of birth								

Place of birth

State		Municipality	
Region		Inhabited place	
Citizenship			

Permanent domicile

State		Street	
Region		Neighbourhood, Block #	
Town (village)		Entrance, Apt. #	
ZIP code		Telephone	

Current domicile

State		Street	
Region		Neighbourhood, Block #	
Town (village)		Entrance, Apt. #	
ZIP code		Telephone	

ID Card	No	issued on date		by	

Place of work

--

name of company

BULSTAT No										
------------	--	--	--	--	--	--	--	--	--	--

Registered office

State		Street	
Town (village)		Office telephone	
ZIP code		Office fax	
Current position			

VII. WHERE THE PERSONS UNDER ITEMS II-VI RESIDE PERMANENTLY ABROAD OR HAVE STAYED ABROAD FOR MORE THAN THREE MONTHS AT A TIME, COMPLETE THE FOLLOWING:

--

Name											

Period	From		To	
	From		To	
	From		To	
State		Exact address		
Reason for stay				

VIII. HAVE YOU BEEN CONVICTED OF A CRIME?

YES											
NO											

When and of what crime

IX. ARE YOU CURRENTLY UNDER INDICTMENT FOR A CRIME?

NO				
YES				

Trial authority and, if available, case No

X. ARE YOU SUFFERING OR HAVE YOU SUFFERED FROM A MENTAL DISORDER?				
NO				
YES				

Specified disorder, duration, institution, attending physician

XI. ARE YOU USING OR HAVE YOU USED DRUGS OR ANY OTHER CONTROLLED PSYCHOTROPIC SUBSTANCES?				
NO				
YES				

Specify substances, duration and current condition (do not specify circumstances where drugs or psychotropic substances were administered to you by qualified physicians, insofar as this did not result in a continued or current taking of such substances)

XII. DURING THE LAST TEN YEARS, HAVE YOU TAKEN, OR ARE YOU STILL TAKING ALCOHOL IN SUCH QUANTITIES AS CAUSE INEBRIATION OR LOSS OF CONSCIOUSNESS?				
NO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
YES	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Specify frequency and circumstances, and whether you are or have been under special therapy in this connection, and if yes, specify institutions and their addresses

XIII. DESCRIBE IN THE TABLE BELOW YOUR OCCUPATION (POSITION) DURING THE LAST TEN YEARS		
Period from... to...	Full Name of Place of Work and Exact Address	Last Position
1.		
2.		
3.		

XIV. DO YOU, OR YOUR SPOUSE OR COHABITANT, HAVE ANY FINANCIAL LIABILITIES TO ANY NATURAL OR LEGAL PERSON EXCEEDING IN AMOUNT SIX TIMES YOUR WAGES?				
NO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
YES	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Specify amount, creditor, repayment period

XV. DO YOU, OR YOUR SPOUSE OR COHABITANT, HAVE ANY OTHER FINANCIAL LIABILITIES (TAXES, MORTGAGES, PLEDGES, MONEY JUDGMENTS)?				
NO				
YES				

Specify liability, amount, beneficiary, payment period

XVI. IF SUCH INFORMATION IS AVAILABLE TO, SPECIFY YOUR INCOME, AND THAT OF YOUR SPOUSE OR COHABITANT, FOR THE LATEST FULL YEAR PRECEDING THE COMPLETION OF THIS QUESTIONNAIRE	

XVII. DO YOU, OR YOUR SPOUSE OR COHABITANT, OWN ANY REAL PROPERTY, COMMERCIAL UNDERTAKING OR INTEREST IN SUCH UNDERTAKING?				
NO				
YES				

XVIII. HAVE YOU EVER HAD ACCESS TO INFORMATION CLASSIFIED AS A STATE SECRET WITHIN THE REPUBLIC OF BULGARIA OR WITHIN ANOTHER STATE OR AN INTERNATIONAL ORGANISATION?				
---	--	--	--	--

NO			
YES			
Period from... to...	State	Full Name and Address of the Organisation within Which You Had Access	Field of Activity (Scope) and Classification Level of the Information Which You Had Access
1.			
2.			
3.			
XIX. AFTER THE AGE OF 18, HAVE YOU STAYED ABROAD FOR MORE THAN TEN DAYS AT A TIME (INCLUDING BUSINESS/OFFICIAL TRIPS)?			
NO			
YES			

State

--

XX. DURING YOUR STAY ABROAD, DID YOU WORK FOR A PAY?

NO			
YES			
Period from... to...	State, Exact Address and Name of Employer	Position	Kind of Work and Income
1.			
2.			
3.			

XXI. DOMICILE AND PERIOD OF DOMICILE DURING THE LAST TEN YEARS (WITHIN THE REPUBLIC OF BULGARIA OR ABROAD)

Period from... to...	State, Inhabited Place, ZIP Code, Street No, Entrance, Floor, Apartment and
1.	

2.			
3.			
XXII. DURING ANY STAY ABROAD, HAVE YOU BEEN INTERROGATED BY ANY FOREIGN AUTHORITY (POLICE, IMMIGRATION, FINANCIAL, ETC) ON SUBJECTS RELATING TO THE COUNTRY'S SECURITY OR DEFENCE? ARE YOU AWARE OF A SIMILAR OCCURRENCE INVOLVING YOUR SPOUSE OR ANY OTHER FAMILY MEMBER?			
NO			
YES			

Do not give any details. These will be discussed with you by a representative of
the investigating authority

XXIII. HAVE YOU EVER BECOME AWARE OF INTEREST IN YOU ON THE PART OF FOREIGN SPECIAL SERVICES, POLICE, BORDER POLICE, OR AN ORGANISED CRIME GROUP (WHETHER BULGARIAN OR FOREIGN)? ARE YOU AWARE OF ANY SUCH INTEREST IN YOUR SPOUSE OR ANY OTHER FAMILY MEMBER?			
NO			
YES			

Do not give any details. These will be discussed with you by a representative of the investigating authority

XXIV. PERSONS, OTHER THAN THOSE UNDER ITEMS II-VI, WHO RESIDE WITH YOU

Name

First name, father's name, family name

Date of birth

Place of birth

State

Municipality

Region

Inhabited
place

Name

First name, father's name, family name

Date of birth

Place of birth

State		Municipality	
Region		Inhabited place	

XXV. OWNER OF YOUR RESIDENCE (IF OTHER THAN YOU)

--

Name, exact address, telephone

XXVI. A. EDUCATION, PROFESSIONAL OR ACADEMIC DEGREES OR DESIGNATIONS

--

XXXVI. B. UNIVERSITIES, SCHOOLS, COURSES ATTENDED

Period from... to...	Name and Address	Certificate No
-------------------------	---------------------	----------------

1.			
2.			
3.			
4.			
XXVII. DO YOU MAINTAIN, OR HAVE YOU MAINTAINED DURING THE LAST THREE YEARS, PERMANENT OFFICIAL OR PERSONAL CONTACTS (FRIENDSHIPS) WITH ANY FOREIGN CITIZENS?			
NO			
YES			
XXVIII. OF WHAT ORGANISATIONS ARE YOU A MEMBER, INCLUDING SEVRET OR INFORMAL ORGANISATIONS AND SOCIETIES?			
Name and Exact Address of Organisation		Position	Period of Membership from..... to
1.			
2.			
3.			

--	--	--	--	--

XXIX. HAVE YOU BEEN AFFILIATED TO THE INTELLIGENCE AND SECURITY SERVICES OF THE PEOPLE'S REPUBLIC OF BULGARIA IN THE MEANING OF THE ACCESS AND DISCLOSURE OF DOCUMENTS AND ANNOUNVCEMENT OF THE AFFILIATION OF BULGARIAN CITIZENS WITH THE STATE SECURITY SERVICE AND THE INTELLIGENCE SERVICES OF THE BULGARIAN PEOPLE'S ARMY ACT

NO		
YES		

XXX. SPECIFY THREE PERSONS WHO HAVE KNOWN YOU FOR MORE THAN THREE YEARS (OTHER THAN THE PERSONS UNDER ITEMS II-VI, OR ANY PERSON SERVING YOUR LEGAL INTERESTS, OR SUCH OTHER PERSON WITH WHOM YOU ARE IN A SPECIAL RELATIONSHIP OF TRUST BY REASON OF SUCH PERSON'S WORK)

Name	Place of work	Exact Address and Telephone
1.		
2.		
3.		

I do declare that I have personally completed the above questionnaire to the best of my knowledge, and I am aware that any deliberate concealment of the truth or representation of an untruth shall be sufficient cause for the termination of my background investigation and that I may be denied clearance for access to classified information by reason of such concealment or representation.

8. In this Questionnaire is to be completed within the time limit prescribed below in connection with your clearance for access to information classified as State secret.

9. The persons under a background investigation for the purposes of clearance for access to information classified as a State secret and marked as "Confidential" must only complete Items: I-VI, VIII, IX, XI-XV, XVIII-XXII, XXIV-XXVI, XXVIII.

10. The persons under a background investigation for the purposes of clearance for access to information classified as a State secret and marked as "Secret" must not complete Item XXX.

11. The persons under a background investigation for the purposes of clearance for access to information classified as a State secret and marked as "Top Secret" must complete all Items.

12. The persons who reapply for clearance for access to information classified as a State secret and marked as "Confidential", upon the expiration of such clearance, must only complete Items: VII, XIII, XVIII-XXI, XXIV, XXVI, and XXVII with data for the period commencing with the date of completion of the previous questionnaire until the date of completion of this Questionnaire. If the relevant data have not changed during that period, enter "No change".

13. The persons who reapply for clearance for access to information classified as a State secret, upon the expiration of the statutory periods, must only complete Items: VII, XIII, XVIII-XXI, XXIV, XXVI, and XXVII, for the period commencing with the date of completion of the previous questionnaire until the date of completion of this Questionnaire. If the relevant data have not changed during that period, enter "No change".

The Protection of Classified Information Act was adopted by the Thirty-Ninth National Assembly on the twenty-fourth day of April twenty-hundred and two, and was promulgated in the State Gazette in pursuance of Decree No. 138 of the 29th of April 2002.

