

STATE SECRETS AND CLASSIFIED INFORMATION OF FOREIGN STATES ACT

Chapter 1

GENERAL PROVISIONS

§ 1. Purpose of Act

The purpose of this Act is to ensure the security and international communication of the Republic of Estonia by protecting state secrets and classified information of foreign states from disclosure or from being accessible to persons who have not been granted access to such information.

§ 2. Scope of application of Act

(1) This Act provides the definition of information which is classified as a state secret, grounds for the expiry of a classification notice for international information, and the bases for classification and the changing of related terms; the grounds for the protection of state secrets, the classified information of foreign states, and classified media and liability incurring from the violation of this Act.

(2) The provisions of the Administrative Procedure Act apply to administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

§ 3. Definitions

In this Act, the following definitions are used:

- 1) “state secret” means information provided for solely in this Act or legislation issued hereunder which requires protection from disclosure in the interests of the national security of the Republic of Estonia or international communication, with the exception of classified information of foreign states;
- 2) “classified information of foreign states” means information originating from a foreign state, the European Union, NATO or other international organisation or an institution established under an international agreement (hereinafter collectively referred to as ‘originator of classified information of a foreign state’) which is communicated to Estonia on the basis of international agreements, and that has been classified as secret by its originator and

information created for the purposes of performance of an international agreement by the Republic of Estonia that is to be classified, as provided by the international agreement;

- 3) “classified medium” means any object which contains a state secret or classified information of foreign states;
- 4) “possessor of classified information” means an agency, constitutional institution or legal or natural person who possesses a state secret or classified information of foreign states;
- 5) “need for access” means the need to process a state secret or classified foreign information if such a need arises from employment or service duties, study or research, or public procurement or international procurement, and also the right to be privy to a state secret or classified foreign information on any other grounds specified in this Act;
- 6) “need-to-know” means the need to access a specific state secret or classified information of foreign states;
- 7) “right for access” means an individual’s right to process state secrets or classified information of foreign states by virtue of office or a decision of a head of an institution, Personnel Security Clearance or Personnel Security Clearance Certificate for Access to Foreign Classified Information, witness protection measures applicable or an order of an investigative body, Prosecutor’s Office or court;
- 8) “processing” means drawing up, marking, collecting, maintaining, preserving, transporting, reproducing, forwarding, destroying or making excerpts of information or medium or being privy to therewith or any other proceedings undertaken with information or medium, regardless of the nature of the proceedings or equipment taken therefore;
- 9) “processing system” means any information system, including any technical equipment which is used for the electronic processing of information;
- 10) “INFOSEC” means the ensuring of the availability, confidentiality and integrity of information (state secrets or classified information of foreign states) in the automated systems processing state secrets or classified information of foreign states;
- 11) “accreditation of processing system” means the evaluation of a processing system against INFOSEC requirements;

- 12) “natural person outside the service” means a natural person who is not a civil servant;
- 13) “national security authority” means a structural unit of the Ministry of Defence, designated under the Statutes of the Ministry of Defence, assigned to organise and supervise the protection of classified information of foreign states;
- 14) “security area” means an area where information classified as ‘confidential’, ‘secret’ or ‘top secret’ or classified information of foreign states and medium containing such information is processed.

§ 4. Authorisation of Permanent Undersecretary

The Minister may authorise the Permanent Undersecretary of the Ministry to conduct any operations and pass decisions that could be conducted and passed by the Minister as a head of an institution under this Act, and also the decisions specified in clause 13 (3) 3) and subsection 27 (5) of this Act.

Chapter 2

STATE SECRETS

Division 1

Levels and Types of State Secrets

§ 5. Classifications of State Secrets

(1) State secrets are protected at the following levels of classification, listed in increasing importance of classification, starting from the lowest level:

- 1) ‘restricted’ level;
- 2) ‘confidential’ level;
- 3) ‘secret’ level;
- 4) ‘top secret’ level.

§ 6. State Secrets Related to Foreign Relations

The following is treated as state secret related to foreign relations:

- 1) items of information concerning international relations, created by a foreign relations institution, except information the disclosure of which would not

damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of fifty years;

- 2) items of information about the import, export and transit of strategic goods, the export of services related to military goods and end-use of strategic goods collected or prepared by the Strategic Goods Commission operating at the Ministry of Foreign Affairs, except information the disclosure of which would not damage security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of thirty years;
- 3) items of information created by a foreign relations institution which, once communicated, would considerably damage international communication of the Republic of Estonia, with the exception of information specified in subsection (1) of this section. Such information shall be classified at the 'restricted' level for a maximum period of fifty years.

§ 7. State Secrets Related to National Defence

The following are treated as state secrets related to national defence:

- 1) items of information concerning the preparation, management and operations of national defence, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of fifty years;
- 2) items of information concerning the preparation and operation of mobilisation, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of thirty years;
- 3) items of information concerning mobilisation stockpile, except information the disclosure of which would not damage the security of the Republic of Estonia or which is subject to disclosure under an international agreement. Such information shall be classified at the 'secret' or lower level for a maximum period of fifteen years;

- 4) items of information concerning military equipment and ammunition of the Estonian Defence Forces and the Defence League, except information the disclosure of which would not damage the security of the Republic of Estonia or which is subject to disclosure under an international agreement. Such information shall be classified at the 'secret' or lower level for a maximum period of thirty years;
- 5) items of information collected by radars and surveillance systems of the Estonian Defence Forces. Such information shall be classified at the 'secret' or lower level for a maximum period of ten years;
- 6) items of information concerning inventions and studies conducted for public defence purposes and their outcome, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of fifteen years;
- 7) items of information collected and synthesised by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 8) items of information concerning the composition, functions and distribution of budget of a structural unit of the Defence Forces which deals with intelligence and counter-intelligence, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of twenty five years;
- 9) items of information concerning the persons and undercover agents recruited for permanent secret co-operation by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence. Such information shall be classified at the 'top secret' level for a maximum period of seventy-five years. Classification shall expire if twenty years have passed since the death of a person specified in this clause but not earlier than fifty years since the classification of the information;

- 10) items of information concerning the collection of covert information by a structural unit of the General Staff of the Defence Forces which deals with intelligence and counter-intelligence, including the information concerning the methods and technical equipment for the collection of information and regarding the objects to be observed, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 11) items of information concerning international co-operation concerning intelligence and counter-intelligence, conducted by the Defence Forces, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 12) items of information concerning the military geography area of the Defence Forces and the Defence League, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years.

§ 8. State Secrets Related to the Maintenance of Law and Order

The following are treated as state secrets related to the maintenance of law and order:

- 1) items of information collected by surveillance agencies when conducting surveillance activities and the methods, tactics and technical equipment used for collection thereof, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years. Classification shall expire upon use of such information in a criminal file or communication thereof to the person with regard to whom the surveillance activities were conducted, or the person whose private or family life was violated by the activities;
- 2) items of information concerning the persons and undercover agents recruited for secret co-operation by surveillance agencies. Such information shall be classified at the 'top secret' or lower level for a maximum period of seventy-five years. Classification shall expire if twenty years have passed since the death of the

person specified in this clause but not earlier than fifty years since the classification of the information;

- 3) items of information concerning police agents of surveillance agencies. Such information shall be classified at the 'restricted' level for a maximum period of seventy-five years. Classification shall expire upon use of such information in a criminal file. Classification of information not included in a criminal file shall expire if twenty years have passed since the death of a person specified in this clause but not earlier than fifty years since the classification of the information;
- 4) items of information concerning the structure, composition and functions of the witness protection sub-unit of the Central Criminal Police, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of fifty years;
- 5) items of information concerning the assets and distribution of the budget of the witness protection sub-unit of the Central Criminal Police, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of thirty years;
- 6) items of information concerning the methods and tactics of the application of witness protection, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 7) items of information concerning witness protection methods and tactics, applied with regard of a specific person, except information the disclosure of which would not damage the safety of the protected person. Such information shall be classified at the 'top secret' or lower level for a maximum period of seventy-five years. Classification shall expire if twenty years have passed since the death of a person specified in this clause but not earlier than fifty years since the classification of the information;
- 8) items of information concerning the national action plan for response in a state of emergency or in war-time, as described in the national crisis management plan,

except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years. Classification shall expire upon public use of such information in an emergency situation or state of war;

- 9) items of information concerning guarded objects subject to serious danger and special requirements applicable to their safety for the purposes of the Security Authorities Act, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level for a maximum period of twenty years;
- 10) items of information concerning the national action plan of the Ministry of Defence and the Ministry of Internal Affairs for response in an emergency situation, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level for a maximum period of twenty years. Classification shall expire upon public use of such information in an emergency situation.

§ 9. State Secrets Related to Security Authorities

The following are treated as state secrets related to security authorities:

- 1) items of information concerning the international co-operation of security authorities, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 2) items of information concerning the assets used by security authorities and distribution of security authorities' budget, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at 'top secret' or lower level for the maximum period of fifty years, except information concerning the buildings and premises used by a security authority, that shall be classified until the expiry of the possession of a building or a premise;
- 3) items of information concerning actions of a security authority in an emergency situation, except information the disclosure of which would not damage the

security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level for a maximum period of twenty years. Classification shall expire upon public use of such information in an emergency situation;

- 4) items of information concerning the collection of covert information by a security authority, including information concerning the methods for the collection of information, except the information specified in subsection 8 (1) of this Act, the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years. Classification shall expire upon use of such information in a criminal file or communication thereof to the person with regard to whom the surveillance activities were conducted, or the person whose private or family life was violated by the activities;
- 5) items of information analysed and synthesised by a security authority when discharging its functions, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 6) items of information concerning the structural units of security authorities or the composition and functions thereof, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'secret' or lower level for a maximum period of fifty years;
- 7) items of information concerning the persons and undercover agents recruited for secret co-operation by a security authority, except the information specified in subsection 8 (1) of this Act. Such information shall be classified at the 'top secret' level for a maximum period of seventy-five years. Classification shall expire if twenty years have passed since the death of a person specified in this clause but not earlier than fifty years since the classification of the information;
- 8) items of information concerning the person who has submitted a personal confession concerning service in a security or intelligence organisation or co-operation therewith to the Security Police Board pursuant to the procedure provided for in clause 5 (2) 1) of the Procedure for Registration and Disclosure of Persons who Have Served in or Co-operated with Intelligence or Counter-

intelligence Organisations of Security Organisations or Military Forces of States which Have Occupied Estonia Act, unless the person who was in the service of the security or intelligence organisation or co-operated therewith committed, in connection with such service or co-operation, an offence which pursuant to the currently valid law of the Republic of Estonia is punishable as a crime in the first degree, or committed crimes against humanity or war crimes and the committing of the crime by the person has been proved by a court with a judgment which has entered into force, or unless the person who was in the service of the security or intelligence organisation or co-operated therewith is the President of the Republic, a member of the Riigikogu² or the Government of the Republic, or a justice of the Supreme Court. Such information shall be classified at the 'secret' level for fifty years. Classification shall expire if twenty years have passed since the death of a person specified in this clause but not earlier than fifty years since the classification of the information;

9) items of information concerning the co-ordination of the activities of security authorities, their co-operation with the Defence Forces and information concerning the Security Committee of the Government of the Republic, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;

10) items of information concerning fictitious persons and bodies impersonated by security authorities and shadow information used, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years.

§ 10. State Secrets Related to Infrastructure and Protection of Information

The following are treated as state secrets related to infrastructure and protection of information:

1) items of information concerning security, alarm, communication and information systems of the Office of the President of the Republic, State Chancellery, security authorities, the Ministry of Defence, the Defence Forces, the Defence League,

the Board of Defence Resources and the Ministry of Foreign Affairs, including the foreign representations and missions, except information specified in clause 2) of this section and information, the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level for a maximum period of thirty years;

- 2) items of information concerning the INFOSEC, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of fifty years;
- 3) items of information concerning buildings and premises used by a structural unit of the Defence Forces which deals with intelligence and counter-intelligence, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level until the expiry of the possession of a building or a premises;
- 4) items of information concerning military equipment and ammunition warehouses of the Defence Forces and the Defence League, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level until the expiry of the possession of a military equipment and ammunition warehouse;
- 5) items of information concerning evacuation of classified medium of a possessor of classified information, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'top secret' or lower level for a maximum period of twenty years;
- 6) items of information concerning the security and alarm systems of a possessor of classified information, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'confidential' or lower level for a maximum period of thirty years.

§ 11. Sub-classes of Information Regarded as State Secrets and the Establishment of its Classification Terms and Levels

- (1) Sub-classes of information specified in § 6, clauses 7 1) – 8) and 10) – 12), clauses 8 1), 2) and 4) – 10), clauses 9 1) – 6) and 9) – 10) and § 10 of this Act and the terms and level of classification of such information shall be established by a regulation of the Government of the Republic. The classification term of sub-classes of classified information may be linked to the occurrence of a particular event, taking into consideration the maximum term of classification specified by this Act.
- (2) The classification level and term specified in subsection 7 (6) of this Act shall be established by the Minister of Defence separately for each invention and study.
- (3) Information specified in § 6, clauses 7 1) – 4), 6), 7) and 10) – 12), clauses 8 1) and 4) – 10), clauses 9 1) – 6) and 9) – 10) and § 10 of this Act, the disclosure of which would not damage the security of the Republic of Estonia, shall be treated as information intended for official use if restriction of access to such information is required under an agreement with a private person, foreign state or international organisation or if disclosure of such information would damage the international communication or discharge of the functions of a possessor of classified information arising from law.

Division 2

Expiry of Classification of State Secrets, Changing the Bases and Term of Classification of Information Classified as State Secret

§ 12. Expiry of Classification of a State Secret

The classification of a state secret shall expire after the expiry of the term of classification, upon the occurrence of a particular event or premature declassification of information classified as a state secret.

§ 13. Premature Declassification of Information Classified as a State Secret

- (1) If information which is classified as a state secret no longer requires protection from disclosure in the interests of national security of the Republic of Estonia, the information is declassified prematurely pursuant to the procedure provided for in this Act.

- (2) Premature declassification of information concerning a natural person specified in clause 7 9), clauses 8 2), 3) and 7) and clauses 9 7) and 8) of this Act, is only permitted during the lifetime of the person concerned upon the written consent of the concerned person and within the extent specified by him or her, except if the person has been convicted of an intentional criminal offence against the state or a crime against humanity.
- (3) The decision to prematurely declassify information which is classified as a state secret is adopted by:
 - 1) the President of the Republic – in the case of a state secret created by the Office of the President of the Republic;
 - 2) the Board of the Riigikogu - in the case of a state secret created by the Chancellery of the Riigikogu and Committees of the Riigikogu;
 - 3) a Minister – in the case of a state secret created within the area of government of the respective Ministry, except a state secret included in a medium submitted to the Government of the Republic or government committee for adopting a decision;
 - 4) the Chief Justice of the Supreme Court – in the case of a state secret created by a court;
 - 5) the Chancellor of Justice – in the case of a state secret created by the Office of the Chancellor of Justice;
 - 6) the Auditor General – in the case of a state secret created by the National Audit Office;
 - 7) the Governor of Eesti Pank – in the case of a state secret created by Eesti Pank or its subsidiaries;
 - 8) State Secretary – in the case of a state secret created by the State Chancellery, except a state secret included in a medium submitted to the Government of the Republic or government committee for adopting a decision;
 - 9) head of a security authority – in the case of a state secret specified in clause 9 4) of this Act. Declassification of information is possible before the intended term of expiry if this is necessary for discharging a function of a security authority and within an extent that will not endanger the

security of individuals who participated or are participating in the collection of the information or who are mentioned in that information.

- (4) The Government of the Republic shall decide on the premature declassification of information which is classified as a state secret not specified in subsection (3) of this section.
- (5) The procedure for filing a request for the premature declassification of information which is classified as a state secret, notification of the intention of premature declassification, contesting premature declassification, notification of premature classification and marking the appropriate medium shall be established by a regulation of the Government of the Republic as provided under the procedure applicable to the protection of a state secret and classified information of foreign states.

§ 14. Procedure for Extension of Term of Classification of Information Classified as a State Secret

- (1) If information which is classified as a state secret also requires protection from disclosure in the interests of the national security of the Republic of Estonia after the expiry of the term of classification provided for in this Act or any legislation passed hereunder, the term of the classification of the information may be extended for five-year periods, but not for more than seventy five years in all. The term of the classification of the information specified in clause 9 8) of this Act may not be extended.
- (2) The decision to extend a term of classification of information which is classified as a state secret is adopted by:
 - 1) the President of the Republic – in the case of a state secret created by the Office of the President of the Republic;
 - 2) the Board of the Riigikogu - in the case of a state secret created by the Chancellery of the Riigikogu and Committees of the Riigikogu;
 - 3) the Chief Justice of the Supreme Court – in the case of a state secret created by a court;
 - 4) the Chancellor of Justice – in the case of a state secret created by the Office of the Chancellor of Justice;

- 5) the Auditor General – in the case of a state secret created by the National Audit Office;
 - 6) the Governor of Eesti Pank – in the case of a state secret created by Eesti Pank or its subsidiaries.
- (3) The Government of the Republic shall decide on the extension of the term of the classification of information which is classified as a state secret not specified in subsection (2) of this section.
- (4) The procedure for filing a request for the extension of the term of the classification of information which is classified as a state secret, notification of the intention of extension of the term of classification, contesting extension of the term of classification, notification of extension of the term of classification, and marking the appropriate medium shall be established by a regulation of the Government of the Republic as provided under the procedure applicable to the protection of a state secret and the classified information of foreign states.

§ 15. Declassification of Information Processed as a State Secret with no Legal Grounds and Changing the Level, Basis and Term of Classification of Information Classified as State Secret

- (1) The Government of the Republic shall declassify the information which is processed as a state secret with no legal grounds or shall change the level, grounds or term of a state secret classified at an incorrect level, on wrong legal grounds or for a wrong term of a state secret included in a medium to be submitted to the Government of the Republic or a government committed for the adoption of a decision.
- (2) A natural person outside the service or institution serving as the originator of the information and in the case of a constitutional institution or legal person, an individual or his/her deputy, assigned as provided in subsection 20 (2) of this Act, shall declassify the information processed as a state secret with no legal grounds or shall change the level, grounds or term of a state secret classified at an incorrect level, on wrong legal grounds or for a wrong term of a state secret, in cases not specified in subsection (1) of this section.

- (3) Should the identification of the originator of the information specified in subsection (2) of this section be impossible or if the originator of the information has ceased to exist, the Minister of Interior Affairs shall declassify the information processed as a state secret with no legal grounds or shall change the level, grounds or term of a state secret classified at an incorrect level, on wrong legal grounds or for a wrong term.
- (4) The procedure for the submission of an application for the declassification of information processed as a state secret with no legal grounds and for changing the level, grounds or term of a state secret classified at an incorrect level, on wrong legal grounds or for a wrong term, notification of the intent of declassifying the information or changing the level of classification, contesting declassification of the information or changing the level of classification, notification of declassification or changing the level of classification and marking of the respective medium shall be established by a regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.
- (5) If the processing of information as a state secret with no legal grounds or the classification of a state secret at an incorrect level, on wrong legal grounds or for a wrong term has been proven by a court ruling or ruling on misdemeanour, the possessors of media bearing such information shall immediately mark such media under the procedure established by the Government of the Republic under subsection (4) of this section.

Protection of State Secrets

Division 1

General Provisions

§ 16. Protection of State Secrets

The protection of state secrets shall be ensured by the following:

- 1) compliance with the procedure for access to state secrets;
- 2) compliance with and assurance of the requirements established for the processing of state secrets and classified media;

- 3) protection of state secrets against unlawful disclosure;
- 4) annual inspection of the existence and integrity of media containing state secrets classified as 'secret' and 'top secret';
- 5) imposition of criminal, misdemeanour or disciplinary liability for violations of the procedure for the protection of state secrets;
- 6) notification of individuals of the requirements for the protection of state secrets before granting access to state secrets.

§ 17. Protection of Classified Media

- (1) A classified medium as a whole is classified at the highest classification level attached to its different parts.
- (2) The term of classification of a medium shall be equivalent to the classification term of a state secret stored on the medium. If state secrets of different types and with different classification terms have been stored on a medium, the term of classification of a medium shall be equivalent to the longest possible term of classification applicable to state secrets stored on the medium.
- (3) The expiry of a classified medium and the term of classification of any excerpts and copies made of this medium shall commence as of the date for the initial registration of a medium as a classified medium.

§ 18. Duty to Maintain State Secrets Applicable to Persons Who Do Not Possess a Right for Access to State Secrets

- (1) A person who does not have the right for access to state secrets but to whom a state secret becomes known or who comes into possession of a classified medium is required to maintain the confidentiality thereof and promptly notify the Security Police Board once realising he or she is in possession of a state secret or classified medium. The person is required to give the classified medium to the Security Police Board.
- (2) If a state secret becomes known to a person specified in subsection (1) or he or she comes into possession of a classified medium by a service or contractual relation, such a person is required to maintain the confidentiality thereof and promptly notify the Security Police Board once having or realising he or she is in possession of a state secret

or classified medium. The person is required to give the classified medium to a person assigned under the procedure specified in subsection 20 (2) of this Act.

(3) In cases specified in subsections 1 and 2 of this section, a person is required to apply reasonable measures at his/her disposal, required to protect classified medium from being disclosed and from access by persons who do not possess a right for access or need-to-know, until a classified medium can be handed over.

§ 19. Duties of Persons with a Right for Access to State Secrets or a Permit to Process State Secrets

A person with a right for access to state secrets or a permit to process state secrets is required to:

- (1) maintain the confidentiality of state secrets which become known to him or her;
- 2) protect classified media in his/her possession from disclosure and access by unauthorised persons who have no right for access or need-to-know;
- 3) notify immediately the agency, constitutional institution or legal person in whose service the person obtained the right for access or a permit to process state secrets due to a service or some other contractual relationship, and the Security Police Board of any person attempting in any way to obtain unlawful access to state secrets;
- 4) notify immediately the agency, constitutional institution or legal person in whose service the person obtained the right for access or a permit to process state secrets due to a service or some other contractual relationship, and the Security Police Board of any attempt to violate the requirements of this Act or any legislation passed hereunder which becomes known to him or her;
- 5) take measures upon illegal disclosure of a state secret or communication thereof to an unauthorised person who has no right for access to avoid the damages potentially resulting from such disclosure or communication;
- 6) notify immediately the corresponding agency which performs security vetting of his/her address and other contact details when staying in a foreign state for a period extending three months;

7) notify immediately the corresponding agency which performs security vetting of his/her name change.

§ 20. Duties of Persons in Possession of a State Secret

- (1) Persons in possession of classified information are required to adopt suitable organisational, physical and INFOSEC security measures for the protection of state secrets.
- (2) The head or directing body of an agency, institution or legal person in possession of classified information is required to appoint a person and the deputy of the person who shall organise the protection of state secrets. If necessary, a structural unit organising the protection of state secrets shall be formed.
- (3) The responsible person or structural unit specified in subsection (2) of this section shall be directly subordinate to the head or directing body of the agency, constitutional institution or legal person, and to the Permanent Undersecretary in ministries, in issues concerning organisation of the protection of state secrets.
- (4) The requirements applicable to the responsible person or structural unit specified in subsection (2) of this section shall be established by a regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.
- (5) The head or a directing body of an institution , a constitutional institution or a legal person in possession of classified information is required to assign positions by classification levels of state secrets, assuming the right for access to state secrets as a prerequisite for holding such a position.
- (6) An institution , a constitutional institution or a legal person in possession of classified information is required to adopt the guidelines for the protection of state secrets, laying down the requirements for the protection of state secrets applicable in a given institution, constitutional institution or a legal person. Requirements to be observed in these

guidelines shall be established by a regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.

(7) The possessor of classified information is required to inspect the existence and integrity of media containing a state secret classified as 'secret' and 'top secret' in its possession at least once per year. The results of the inspection shall be recorded in writing.

(8) Classified media shall be deposited with the Security Police Board or, in the case of the Defence League or the Defence Forces, given to the General Staff of the Defence Forces upon the closure of an institution, a constitutional institution or a legal person in possession of classified information.

§ 21. Use of a Weapon for the Protection of a State Secret

(1) A military or a service weapon may be used for the protection of a state secret if the danger cannot be diverted in another way or in time. One must do everything possible to avoid threatening a life or the physical integrity of any third party when using a weapon.

(2) One may use a firearm against a person only as an extreme measure to render the attacker incapable of attack, resistance or escape for protecting state secrets classified as 'confidential', 'secret' or 'top secret', if no other option is available for the protection of state secrets and it is necessary, at the same time, to:

- 1) fend off an immediate threat to one's life or the danger of serious physical harm occurring;
- 2) prevent the escape of a person if that person is in illegal possession of a media containing a state secret classified as 'secret' or 'top secret', or
- 3) prevent the commitment of a crime of a first degree that can be anticipated or is in process or the commitment of a crime that may result in a life sentence in prison.

(3) A person against whom a weapon shall be used must be first warned of the use of a weapon. Should the warning give no result or is not possible due to the

urgent need to fend off a threat or dominant need to protect some benefits, one is free to use a weapon.

§ 22. Competence of Security Police Board and General Staff of Defence Forces in Organising the Protection of State Secrets

- (1) The protection of state secrets shall be organised and supervision over implementation of this Act and any legislation passed hereunder shall be exercised by the Security Police Board, and in the Defence Forces and the Defence League, by the General Staff of the Defence Forces, except in the cases specified in § 23 of this Act.
- (2) The Security Police Board and the General Staff of the Defence Forces are required, as appropriate, to:
 - 1) supervise the compliance with requirements of state secret protection in agencies, constitutional institutions and legal persons in possession of classified information, and supervise the access by natural persons to state secrets;
 - 2) supervise compliance with requirements of the processing of state secrets and classified media;
 - 3) determine violations of requirements of this Act or any legislation passed hereunder;
 - 4) make proposals to the Security Committee of the Government of the Republic for the prevention and elimination of the deficiencies and violations;
 - 5) organise periodic training on issues of the protection of state secrets;
 - 6) check for the presence of illegal intercept devices in a security area of classified information of a possessor of classified information, depending on the risk assessment rating.
- (3) In the course of exercising supervision, the Security Police Board and the General Staff of the Defence Forces have the right for access to all necessary information and issue mandatory precepts to the possessor of classified

information for the elimination of a violation or danger of violation of requirements arising from this Act or any legislation passed hereunder.

- (4) If, in the course of supervision, violations of requirements established by this Act or legislation issued on the basis thereof are ascertained which may bring about a disclosure of state secrets, the Security Police Board and the General Staff of the Defence Forces, as appropriate, have the right to issue a mandatory precept to the possessor of state secrets who is being supervised for the suspension of the processing of classified information and, if necessary, to take the classified media temporarily into storage until establishment of the necessary conditions.
- (5) Upon failure to comply with the precept, specified in clauses 3) and 4) of this section, the Security Police Board and the General Staff of the Defence Forces may impose a penalty payment with a maximum value of 50,000 EEK.
- (6) The working schedule for the conduct of inspection of state secret protection by the Security Police Board and working procedure of the Committee conducting inspection shall be approved by the Minister of Internal Affairs.

§ 23. Competence of Information Board in Organising the Protection of State Secrets

(1) The Information Board shall:

- 1) organise and verify compliance with the requirements established for INFOSEC;
- 2) organise and verify the protection of state secrets on foreign missions and in the units of the Defence Forces located outside the territory of the Republic of Estonia.

(2) The Information Board shall, for the purpose of organisation and verification of INFOSEC:

- 1) provide advice and guidance to possessors of classified information in matters related to INFOSEC for the protection of state secrets;
- 2) provide advice and guidance to possessors of classified information in matters related to the violation of requirements established for INFOSEC, participate in the assessment of incurred damages, give recommendations for the adoption of additional security measures;

- 3) initiate the accreditation of a processing system at the request of a possessor of classified information or at its own initiative;
- 4) issue and invalidate a statement of accreditation given to a processing system and interim approval to operate;
- 5) co-operate with foreign states and international organisations in matters related to INFOSEC;
- 6) organise and verify the processing of encrypted materials that are used to protect state secrets and provide advice and guidance for their processing;
- 7) adopt security measures to protect the processing system against security failure or the threat for its incurrence;
- 8) organise periodic training for assuring conformity with INFOSEC requirements;

(3) The Information Board shall perform the following functions in foreign missions and in the units of the Defence Forces located outside the territory of the Republic of Estonia:

- 1) supervise the compliance with requirements of state secret protection and access by natural persons to state secrets;
- 2) supervise compliance with requirements for the processing of state secrets and classified media;
- 3) determine violations of requirements of this Act and legislation issued on the basis thereof;
- 4) make proposals to the Security Committee of the Government of the Republic for the prevention and elimination of deficiencies and violations;
- 5) organise periodic training on issues of the protection of state secrets;
- 6) check for the presence of illegal intercept devices in a security area of classified information of a possessor of classified information, depending on the risk assessment rating.

(4) In the course of exercising supervision, the Information Board has the right for access to all necessary information and issue mandatory precepts to the possessor of classified information for the elimination of a violation or danger of violation of requirements arising from this Act or any legislation passed hereunder.

(5) If, in the course of supervision, violations of requirements established by this Act or legislation issued on the basis thereof are ascertained which may bring about a disclosure of state secrets, the Information Board has the right to issue a mandatory precept to the possessor of state secrets who is being supervised for the suspension of the processing of state secrets and classified media, if necessary, to take the classified media or a part of a processing system temporarily into storage until establishment of the necessary conditions.

(6) If the Information Board imposes the penalty fine upon the failure to comply with the precept, specified in clauses 4) and 5) of this section, the maximum amount of the penalty fine to be imposed is 50,000 EEK.

§ 24. Competence of the Security Committee of the Government of the Republic in Organising the Protection of State Secrets

The Security Committee of the Government of the Republic shall:

- 1) provide advice to the Government of the Republic for the organisation of the protection of state secrets;
- 2) review petitions and complaints concerning the unlawful application of or failure to apply this Act or legislation issued on the basis thereof by a minister or the Commander of the Defence Forces, and shall inform the Government of the Republic of the results of the review;
- 3) give an opinion concerning draft legislation and international agreements pertaining to state secrets submitted to the Government of the Republic;
- 4) express opinion concerning premature declassification of state secrets, extension of term of classification and the grounds, level and term of classification.

Division 2

Access to State Secrets

Sub-Division 1

General Provisions

§ 25. Granting Access to State Secrets

- (1) Before permitting access to a state secret, the possessor of classified information is required to ascertain each time that the person holds a Personnel Security Clearance of the corresponding classification and verify that the person has a need-to-know.
- (2) If classified medium contains state secrets classified at different levels, other information with restricted access or information not subject to restricted access, access shall be granted to the part of medium not containing information with restricted access or to information made available to that respective person according to right for access and need-to-know. Access is denied to the part of medium that provides the basis for drawing conclusion on the part of the medium to which the person holds no right for access or need-to-know.
- (3) A citizen of a foreign state, a person with no citizenship or a legal person registered in a foreign state may only be granted access to a state secret in the following cases:
 - 1) for the participation of a person in negotiations concerning a public or international procurement;
 - 2) a possessor of classified information needs to grant the person access in connection with functions to be discharged by the institution and the person concerned has the required special knowledge, skills or equipment to contribute to discharging the aforementioned functions, or
 - 3) in cases specified in § 29 or § 30 of this Act.

Sub-Division 2

Right for Access

§ 26. Right for Access to State Secrets

- (1) A person has the right for access to state secrets:
 - 1) by virtue of office;
 - 2) under the decision of a head of an agency;
 - 3) under a Personnel Security Clearance;

- 4) in relation to the adoption of witness protection measures or
 - 5) by the ruling of an investigation institution, prosecutor's office or court.
-
- (2) A Personnel Security Clearance to a higher classification of state secrets also grants the right for access to a lower classification of state secrets. A Personnel Security Clearance to a lower classification of state secrets does not grant the right for access to a higher classification of state secrets.
 - (3) Right for access is not granted solely with the purpose of granting a person access to a security area of classified information or to facilitate movement in the security area.
 - (4) A processing permit does not grant the person holding the permit under contractual or service relationship right for access to state secrets.
 - (5) The term of right for access, granted in case of temporary need for access, must not exceed the term of the person's participation in the temporary task or work.
 - (6) Expiry of right for access to state secrets does not relieve the person who held a right for access from the obligation to maintain the confidentiality of a state secret.
 - (7) The person who held a right for access must return all the classified media in his/her possession to the possessor of classified information, which granted him or her access to state secrets, upon the expiry of the right for access. Media that only contain state secrets created by the person who held the right for access are handed over to the agency that initiated the creation of information and to the Security Police Board in all other cases.

§ 27. Right for Access to State Secrets by Virtue of Office and Under the Decision of a Head of an Agency

- (1) Right for access to any level of state secret is, under this Act, given by virtue of office to the following individuals:
 - 1) President of the Republic;
 - 2) member of the Riigikogu;

- 3) member of the Government of the Republic;
- 4) a judge;
- 5) Commander and Commander-in-Chief of the Defence Forces;
- 6) Chancellor of Justice and Deputy Chancellor of Justice-Adviser;
- 7) Auditor General;
- 8) Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank.

(2) Right for access only to state secrets classified as 'restricted' shall be granted, by virtue of office, to civil servant of a state agency or an employee of Eesti Pank, chosen or hired for an office that requires access to state secrets classified as 'restricted' as a prerequisite for holding this office.

(3) If circumstances specified in subsection 32 (1) of this Act are revealed concerning the person applying for or holding the office specified in subsection (2) of this section:

- 1) this person will not be given an office that requires access to state secrets; or
- 2) this person is dismissed from an office that requires access to state secrets under the procedure provided by the Public Service Act or some other specific legal act, regulating public services or the contract of employment, signed with this person, is terminated, as provided in the Employment Contracts Act of the Republic of Estonia.

(4) If circumstances specified in subsection 32 (1) of this Act are revealed concerning the person applying for or holding an office that assumes access to state secrets classified as 'restricted', specified in subsection (2) of this Article, the head of a security authority, who conducts security control on the person, may deprive the person of the right for access to state secrets classified as 'restricted' or refuse to grant the right until the appropriate circumstances have lapsed. Clauses (3) 1) and 2) of this section shall be applicable in this case.

(5) The decision to grant natural persons outside the services, except the employees of Eesti Pank, the right for access only to a state secret classified as 'restricted', is adopted separately in each case by:

- 1) the appropriate minister;
- 2) the head of the appropriate institution in the case of the Chancellery of the Riigikogu, Office of the President, State Chancellery, Office of the Chancellor of Justice, Eesti Pank, courts and State Audit Office;
- 3) the Governor of Eesti Pank in Financial Supervision Authority.

(6) The right for access shall be granted for a fixed term in cases specified in subsection (5) of this section. The right for access expires upon the expiry of the fixed term, if not extended, or upon the deprivation of right for access.

(7) If circumstances specified in subsection 32 (1) are revealed regarding the person specified in subsection (5) of this section, the person shall be denied the right for access to state secrets classified as 'restricted', or the right for access shall be deprived with the decision of a person competent to cancel the right for access.

(8) If circumstances specified in subsection 32 (2) are revealed regarding the person specified in subsection (5) of this section, the head of a security authority, who conducts security control on the person, may deprive the person of the right for access to state secrets classified as 'restricted' or refuse to grant the right until the appropriate circumstances have lapsed.

(9) The security authority shall send the officially verified transcript of a decision, specified in subsections (4) and (8) of this section, within five working days to a person who was deprived of the right for access and a notice regarding the adoption of such a decision to an agency, constitutional institution or a legal person, which employs the person or which granted the right for access to the concerned person.

(10) If a person applying for or holding a right for access only to a state secret classified as 'restricted' holds no right for access to state secrets classified as 'confidential', 'secret' or 'top secret', the agency specified in subsections (2) or (5) of this section shall:

- 1) notify the person who has been granted the right of access of the obligations, specified in § 19 of this Act;

- 2) shall take a signed verification of the person, stating that he or she is aware of the requirements for the protection of state secrets, liability incurring from their violation, and obligation to safeguard the state secret becoming known to him or her;
 - 3) shall take a signed consent from the person that shall entitle an agency competent to conduct security verification information concerning the person from natural and legal persons and from institutions and bodies for the adoption of a decision concerning both the granting of the right for access or extending its term and during the term of the right for access.
- (11) Verification and consent, specified in subsection (10) of this section, are taken for the agency competent to conduct security verification information concerning the person.
- (12) Should the person refuse to give their verification or consent, specified in subsection (10) of this section, the person shall be not granted the right for access only to state secrets classified as ‘restricted’. Subsection (3) of this section shall be applicable to a person, who applies for or holds an office requiring the right for access to state secrets classified as ‘restricted’.
- (13) The format of the documents specified in clauses (10) 2) and 3) of this section is established by a regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.

§ 28. Right for Access to State Secrets under Personnel Security Clearance

- (1) The right for access to state secrets classified as ‘confidential’, ‘secret’ or ‘top secret’ is available to a natural person holding a Personnel Security Clearance (hereinafter the ‘Personnel Security Clearance’) of an appropriate level.
- (2) If provided under an international agreement, application of a Personnel Security Clearance is not required from a citizen of a foreign state or a person with no citizenship, who holds a right for access to the appropriate level of classified information of a foreign state.

§ 29. Right for Access to a State Secret on the Basis of a Reasoned Order of an Investigative Body or Prosecutor's Office or a Court Ruling

- (1) Participants in pre-trial proceedings or judicial proceedings in criminal, civil or administrative matters, or matters of misdemeanour have the right for access, after passing security vetting, to state secrets classified as “restricted”, “confidential” or “secret” on the basis of a reasoned order of an investigative body, Prosecutor's office or a court ruling if access is unavoidably necessary for the adjudication of the criminal, civil or administrative matter, or the matter of misdemeanour.
- (2) Access on the basis of a reasoned order from an investigative body, Prosecutor's office or a court ruling is not permitted to state secrets classified as “restricted”, “confidential” or “secret” if this endangers the performance of the duties provided for in clauses 8 (1) 2), 3) or 4) of the Surveillance Act, or to state secrets classified as “top secret”.
- (3) Security vetting shall not be performed in respect of suspects, the accused, accused at trial and a counsel who is an advocate if the need to access state secrets arises from ensuring the right of defence in criminal proceedings.
- (4) An investigative body, Prosecutor's office or court shall forward an application for the conduct of security vetting to an agency which performs security vetting prior to the decision on the granting of the right for access to state secrets to a person. In order to pass security vetting, the person shall submit the document specified in clause 27 (10) 3) of this Act to the agency which performs security vetting.
- (5) The agency which performs security vetting shall present the information obtained as a result of security vetting to an investigative body, Prosecutor's office or court within the term specified thereby, and this term shall not be less than one month.
- (6) A an investigative body, Prosecutor's office who prepared an order or a court which prepared a ruling shall notify the person to be granted a right for access to state secrets pursuant to the procedure prescribed in this section of the obligations specified in § 19 of this Act, and shall obtain a signed confirmation

described in subsection 27 (10) 2) of this Act from a person who is granted access to state secrets before access to the information is granted, which shall be included in the materials of the file.

- (7) If the person refuses to sign the consent, specified in subsection (4) of this section or a confirmation specified in subsection (6) of this section, the consent or confirmation shall contain a notation concerning the refusal and the reasons therefore and shall be confirmed by the body conducting proceedings. The person who refuses to give the consent or confirmation shall not be granted the right for access to state secrets.

§ 30. Right for Access to State Secrets of Persons Protected Under the Witness Protection Act and Their Representatives

- (1) A person in respect of whom witness protection measures are applied pursuant to the Witness Protection Act and the advocate representing the aforementioned person have the right for access to state secrets concerning his/her protection without a Personnel Security Clearance or compliance with the requirement to pass security vetting, to an extent which is unavoidably necessary. The person shall be notified of the obligations provided for in § 19 of this Act and is required to sign the confirmation, specified in subsection 27 (10) 2) of this Act. The person refusing to give the confirmation shall not be granted the right for access to state secrets.
- (2) A representative of the person specified in subsection (1) of this section, not being an advocate, is given access to state secrets concerning the protection of the aforementioned person after passing security vetting, to an extent which is unavoidably necessary. Subsections 29 (4) – (7) of this Act are applicable to such cases.

Sub-Division 3

Application for Issue, Issue, Extension of Term and Expiry of a Personnel Security Clearance

§ 31. Application for Personnel Security Clearance or Extension of Term Thereof

(1) In order to obtain a Personnel Security Clearance or to be granted extension of the term thereof, a person shall submit an application to the agency which performs security vetting through a constitutional institution, governmental authority or state agency administered by a government authority (hereinafter the 'supporter of Personnel Security Clearance') which justifies the need for access and supports the receipt or extension of the term of the Personnel Security Clearance, to which the following documents shall be appended:

- 1) a letter from the supporter of the Personnel Security Clearance (except if the supporter of the Personnel Security Clearance and agency performing security vetting are one and the same agency) which justifies the need for access by the person who is in an employment, service or contractual relationship or applying for such relationship and which supports the receipt of a Personnel Security Clearance or extension of the term thereof;
- 2) a completed form filled in by the applicant upon application for Personnel Security Clearance or, upon extension of the term of Personnel Security Clearance within the period of one year as of the expiry of the previous Personnel Security Clearance, a completed annex to the form;
- 3) documents specified in clauses 27 (10) 2) and 3) of this Act.

(2) Upon extending the term of Personnel Security Clearance, one may, if applicable, apply for access to state secrets of a classification level lower or higher than specified in the valid Personnel Security Clearance.

(3) Documents for the grant of the extension of the term of a Personnel Security Clearance shall be submitted to the agency which performs security vetting not later than three months before the expiry of the Personnel Security Clearance.

(4) The term of a Personnel Security Clearance shall be extended until the decision to extend or to refuse from reviewing the application has been adopted in the case of the timely submission of documents required to be granted an extension of the term of a Personnel Security Clearance.

- (5) The format of the application for a Personnel Security Clearance or extension of the term thereof and the format of an application form and the annex thereto shall be established by a regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.

§ 32. Bases for Refusal to Issue Personnel Security Clearance or Extend Term Thereof

(1) A Personnel Security Clearance shall not be issued to or extension of the term thereof shall be refused for natural persons:

- 1) who are lacking the need-to-know;
- 2) who do not meet the requirements provided for in subsection 33 (1) of this Act;
- 3) with restricted active legal capacity;
- 4) who are employed by the intelligence or security service of a foreign state, except if the person complies with the requirements specified in subsection 25 (3) of this Act and does, according to a security authority, not pose a threat to the security of the Republic of Estonia;
- 5) who have been disclosed or are subject to disclosure pursuant to the procedure provided for in the Procedure for Registration and Disclosure of Persons who Have Served in or Co-operated with Intelligence or Counter-intelligence Organisations of Security Organisations or Military Forces of States which Have Occupied Estonia Act;
- 6) who are serving a prison sentence;
- 7) whose activities are directed against the Estonian state and its national security;
- 8) who have been punished for committing an offence against the state or humanity regardless of whether the punishment has not been expunged from the punishment register or not;
- 9) who have been deprived of the right for access due to violation of the provisions of this Act and legislation issued on the basis thereof;
- 10) whose previously issued Personnel Security Clearance has been revoked due to violation of the provisions of the State Secrets Act (RT I 1999, 16, 271; 2005, 64, 482) or legislation issued on the basis thereof within the period of five years as of the revocation of Personnel Security Clearance.

(2) Issue of a Personnel Security Clearance or extension of the term thereof may be refused for natural persons:

- 1) whose activities have been directed against the Estonian state and its national security;
- 2) who are involved with an organisation which by its activities ignores public policy or the purpose of which is to change the independence of the Republic of Estonia by violence, violent breach of territorial integrity, violent seizure of power, or violent changing of the constitutional order of Estonia;
- 3) who are participants in criminal proceedings as suspects or accused;
- 4) who have been punished several times for misdemeanours and information concerning the punishment has not been expunged from the punishment register;
- 5) who have been punished for intentionally committed official misconduct or a corruptive act, regardless of whether the punishment has not been expunged from the punishment register or not;
- 6) against whom disciplinary proceedings or misdemeanour proceedings with elements of official misconduct or corruption or violation of this Act or any legislation issued on the basis thereof are conducted;
- 7) who have been punished for an intentionally committed criminal offence if information concerning the punishment has not been expunged from the punishment register;
- 8) who have been punished for committing a criminal offence against the state due to negligence, regardless of whether the punishment has not been expunged from the punishment register or not;
- 9) who are dependent on narcotic or psychotropic drugs or alcohol or gambling;
- 10) who have concealed information or submitted falsified or false information which is essential in deciding on the issue of the Personnel Security Clearance on the form or annex thereto submitted to the agency which performs security vetting or in the interview for applicants for Personnel Security Clearances;
- 11) who have not performed all of their obligations regarding state and local taxes;
- 12) who have stayed in a foreign state for a longer period for circumstances that cannot be identified;

- 13) who suffer from mental disturbances that limit their ability to understand or control their behaviour;
- 14) who are economically dependent on their spouse, grandparent, parent, brother, sister, child or grandchild, in respect of whom the circumstances provided for in clauses (1) 4) 5) and 7), or clause (2) 2) of this section become evident;
- 15) who have, either by word or deed, expressed dishonesty, disloyalty, untrustworthiness or indiscretion that may refer to the person's untrustworthiness to protect a state secret.

(3) Security vetting shall be performed on the person under the provisions of this Act to check the circumstances specified in subsections (1) and (2) of this section.

(4) If circumstances provided for in subsection (1) or (2) of this section become evident in respect of a person, an agency, constitutional institution or legal body which is in an employment, service or contractual relationship with the person is required to promptly notify thereof the agency competent to perform security vetting with respect to the person.

§ 33. Issue of Personnel Security Clearance and Extension of Term Thereof

- (1) A Personnel Security Clearance may be issued to a citizen of Estonia or a natural person specified in subsection 25 (3) of this Act.
- (2) The basis for issue of a Personnel Security Clearance or extension of the term thereof is a decision which is made on the basis of security vetting and which shall be founded on all the information gathered in the course of security vetting.
- (3) Issue of a Personnel Security Clearance or extension of the term thereof shall be decided by a head of an agency which performs security vetting no later than within three months as of the receipt of documents required for the issue of an Personnel Security Clearance or extension of the term thereof. A Personnel Security Clearance shall be issued by an agency which has conducted security vetting with respect to the person.

(4) An agency which performs security vetting may extend the term described in subsection (3) of this section by three months in the following cases:

- 1) where it has not been possible to conduct an interview with the applicant for a Personnel Security Clearance in the course of security vetting within the period of three months as of the submission of the required documents due to material circumstances depending on the applicant;
- 2) where it is necessary for the decision on the granting of a Personnel Security Clearance to be based on information originating from a foreign state;
- 3) where information gathered in the course of security vetting indicates that bases for refusal to issue a Personnel Security Clearance are likely to become evident within the following three months;
- 4) where information gathered in the course of security vetting indicates that bases for refusal to issue a Personnel Security Clearance may cease to exist in respect of the person subject to security vetting within the following three months.

(5) An agency which performs security vetting shall refuse to review the application in the following cases:

- 1) where it has not been possible to conduct an interview with the applicant for a Personnel Security Clearance in the course of security vetting within the period of three months as of the submission of required documents due to immaterial circumstances depending on the applicant;
- 2) the granting of a right for access or extension of the term thereof to state secrets classified at the same or lower level has been refused to this person earlier and the application does not show that the circumstances serving as the grounds for refusal have lapsed;
- 3) upon the application of the applicant of Personnel Security Clearance or his/her supporter;
- 4) in other situations provided by law.

(6) If a Personnel Security Clearance to the classification level of state secrets specified in the application cannot be issued to a person or extension of the term thereof is not possible as the result of the consideration of circumstances specified in subsection 32 (2), but it would be possible to issue or extend the

term of a Personnel Security Clearance to a lower level of classification, a Personnel Security Clearance is issued or extension of the term thereof is granted for a lower level of classification, if considered necessary by the applicant for the Personnel Security Clearance and his/her supporter.

- (7) In order to access state secrets classified as 'top secret' or 'secret', a Personnel Security Clearance shall be issued to a person for up to five years or the term thereof shall be extended for up to five years. In order to access state secrets classified as "confidential", a Personnel Security Clearance shall be issued to a person for up to seven years or the term thereof shall be extended for up to seven years.
- (8) If the issue of a Personnel Security Clearance is applied by a person who wishes to hold an office where access to state secrets is a prerequisite for employment or who wants to enter into an agreement where access to state secrets is a prerequisite for the performance of the agreement, the Personnel Security Clearance issued shall be validated as of the moment of the appointment or assignation of the person for the office or as of the enforcement of the appropriate provision of the contract. The term of the Personnel Security Clearance is then calculated as of the date for issue of the Personnel Security Clearance.
- (9) A Personnel Security Clearance or extension of the term thereof shall be prepared on the letter-head with security features of the agency which performs security vetting, with the signature of the head of the agency. A Personnel Security Clearance or a notice concerning extension of the term thereof shall set out the following data:
 - 1) the date of issue of the Personnel Security Clearance or extension of the term thereof and the number of the decision;
 - 2) the basis for the decision;
 - 3) the given name, surname, personal identification code, and job or position of the person;
 - 4) the classification of state secrets which the person is permitted to access;
 - 5) the term of the Personnel Security Clearance.

- (10) A notice concerning the issue of the Personnel Security Clearance or extension of the term thereof shall be sent to the applicant within five working days as of the adoption of the decision through the supporter of the Personnel Security Clearance.
- (11) Upon refusal to issue a Personnel Security Clearance or extend the term thereof, the agency which performs security vetting shall send an officially certified copy of the decision to refuse to issue the Personnel Security Clearance or extend the term thereof to the applicant for a Personnel Security Clearance and a notice concerning the decision to refuse to issue the Personnel Security Clearance or extend the term thereof to the supporter of the Personnel Security Clearance within five working days as of the adoption of the decision, except if the supporter is the agency performing security vetting.
- (12) If a person holding an office where access to state secrets is a prerequisite for employment or applying for such an office is refused the issue of the Personnel Security Clearance or the extension of the term thereof, provisions of clauses 27 (3) 1) and 2) of this Act shall apply.

§ 34. Expiry of Personnel Security Clearance

- (1) A Personnel Security Clearance shall expire:
- 1) upon the death of a person or upon a person being declared dead or as missing by a court ruling;
 - 2) upon expiry of the term specified in a Personnel Security Clearance;
 - 3) upon revocation of a Personnel Security Clearance;
 - 4) revocation of the right for access from a person with an enforced court judgment or the decision of a body conducting extrajudicial proceedings.
- (2) A Personnel Security Clearance, issued to a person, is declared invalid if circumstances specified in subsection 32 (1) of this Act become evident with respect to that person.
- (3) A Personnel Security Clearance, issued to a person, may be declared invalid if circumstances specified in subsection 32 (1) of this Act become evident with respect to that person.

- (4) In the case of a short-term lapse in the need for access, a Personnel Security Clearance need not be revoked.
- (5) The person that has the competence to decide the extension of the term of a Personnel Security Clearance held by the person shall revoke a Personnel Security Clearance.
- (6) The agency that supports the issue of the Personnel Security Clearance and an agency, constitutional institution, or a legal body, in which a natural person whose Personnel Security Clearance is revoked is employed or contracted by, shall promptly be notified of the revocation of the Personnel Security Clearance of the natural person.
- (7) The agency which performs security vetting shall immediately inform the national security authority of the expiry of the term of a Personnel Security Clearance of a person holding an Personnel Security Clearance Certificate for Access to Foreign Classified Information on the basis of clauses (1) 3), 4) or 5) of this section.
- (8) If a person holds an office where access to state secrets is a prerequisite for employment or is applying for such an office is refused the issue of the Personnel Security Clearance or the extension of the term thereof or the invalidity of the Personnel Security Clearance is identified, the provisions of subsection 27 (3) of this Act shall apply.

Division 3

Processing of State Secrets and Classified Media

Sub-Division 1

General Provisions

§ 35. Communication of State Secrets

- a. Internally, state secrets communicated to a possessor of classified information may only be communicated upon the written consent of a head or directing body of an agency, constitutional institution, or public legal person who is the originator of the state secret or, in the case of a

state secret related to criminal proceedings, the prosecutor in charge of the proceedings or a prosecutor above him, observing the procedure specified in this Act and legislation issued on the basis thereof. If a natural person outside a service or a legal person governed by private law is an originator of the information, a supporter of Personnel Security Clearance or processing permit shall also give a written consent for communication of the information.

- b. If the originator of information, specified in subsection (1) of this section, cannot be identified or the originator of the information or an agency supporting the issue of access or processing permit has ceased to exist, consent for communication is given by the Minister of Internal Affairs.
- c. Provisions of subsection (1) and (2) of this section shall not apply upon the communication of state secrets within an agency, constitutional institution, or legal person, also when communicating state secrets to authorities specified in § 22 and § 23 of this Act, national security authority, a court, the Riigikogu, the Chancellor of Justice, the Auditor General, and the Government of the Republic.
- d. State secrets may be communicated to a foreign state, international organisation, or an institution established under an international agreement by the State Chancellery, Ministry of Defence, Ministry of Internal Affairs, Ministry of Foreign Affairs, and a security authority, observing the procedure specified in this Act and legislation issued on the basis thereof, if this is necessary to assure or increase the security of the Republic of Estonia under an international agreement and if the agency receiving the information shall ensure the protection of communicated information from disclosure.
- e. State secrets may be communicated to a foreign state or an international organisation by the Central Criminal Police, observing the procedure specified in this Act and legislation issued on the basis thereof and provisions of the Witness Protection Act, provided that the agency receiving the information shall ensure the protection of communicated information from disclosure.

- f. Communication of state secrets to a foreign state, international organisation or an institution established under an international agreement shall be first registered at national security authority, except if information is being communicated by a security authority or the Criminal Police under the provisions specified in this section.

§ 36. Maintaining Records of Classified Media

- (1) Maintaining records of classified media is performed as provided by the Administrative Procedure Act, Archives Act, regulation of the Government of the Republic adopted under subsection 58 (1) of the Public Information Act and legislation issued on the basis thereof, considering the specificities provided by this Act and legislation issued on the basis thereof.
- (2) Registration of copies made of classified media, except media containing state secret classified as ‘restricted’ or ‘confidential’, is mandatory.
- (3) The Government of the Republic may lay down requirements different from provisions specified in subsection (2) of this section for the registration of electronic classified media, observing the procedure applicable to the protection of a state secret and classified information of foreign states procedure.

§ 37. Marking of Classified Media

- (1) Classified media shall be marked with:
 - a. a classification marking;
 - b. a notation concerning the legal basis for classification of the information;
 - c. a notation concerning the date of registration and term of classification of media
- (2) Classified media may be left unmarked only if marking may endanger the classification of state secret.
- (3) Classified media shall be marked only as follows:
 - 1) a classified medium containing a state secret classified as “restricted” shall be marked with a classification marking “PIIRATUD” [*restricted*];

- 2) a classified medium containing a state secret classified as “confidential” shall be marked with a classification marking “KONFIDENTSIAALNE” [*confidential*];
 - 3) a classified medium containing a state secret classified as “secret” shall be marked with a classification marking “SALAJANE” [*secret*];
 - 4) a classified medium containing a state secret classified as “top secret” shall be marked with a classification marking “TÄIESTI SALAJANE” [*top secret*].
- (4) Media containing state secrets that also contains classified information of foreign states, shall be marked with information concerning the processed classified information of foreign states, if provided by an international agreement.
- (5) Should it be expedient to mark classified media additionally by paragraphs and illustration, the marking of a paragraph is inserted into the beginning and end of each paragraph and illustration. Unmarked paragraphs and illustrations, present in a media with a paragraph marking, are given the classification level of the media, until the originator of information has decided how the appropriate paragraph or illustration should be marked. Marking must be decided promptly after the need for processing of that respective paragraph or illustration incurs.
- (6) Classified media may be marked by additional marking that refers to additional security measures applicable to media or circle of persons, which has the right for access to the media.
- (7) If media is marked with a classification marking, the possessor of the classified media is required to put an appropriate marking on the classified media upon the expiry of the classification term applicable to state secrets.

§ 38. Storage and Destruction of Classified Medium

- (1) A medium the term of classification of which has expired shall be transferred to the National Archives in accordance with the Archives Act.
- (2) Part of media, containing sensitive personal data, transferred to a media the classification term of which has been expired and that contains information collected as the result of collection of information or covert investigation, shall not be transferred to the National Archives if a person in regard to whom the surveillance activities were conducted, or the person whose private or family life

was violated by the activities requests the destruction of information containing sensitive personal data and this information is no longer required for public purposes. In such cases, the part of media that contains sensitive personal data shall be destroyed in a way that shall make the restoring of the information contained impossible.

(3) In the case of media, the classification of which has not expired, it shall only be allowed to destroy:

- 1) a copy made of classified media;
- 2) a classified media in an unexpected situation where there is no other alternative available to protect the media from access by a person not having the right for access and such access would probably result in considerable damages to the security of the Republic of Estonia. In such cases, the originator of the classified information, having created the medium, Security Police Board and Security Committee of the Republic of Estonia shall be promptly notified of the destructions and the reasons thereof;
- 3) a draft after the compilation of a medium that the draft was prepared for;
- 4) a medium with no archival value upon the consent of the state archivist or an official authorised by him/her;
- 5) a medium which is not a record for the purposes of the Archives Act;
- 6) a classified medium that only contains classified information of a foreign state and that has not been assigned a storage term by the originator of the classified information of foreign states or the destruction of which is not prohibited under an international agreement;
- 7) a medium that contains only the information specified in § 10 of this Act.

(4) In cases specified in subsection (3) of this section, the classified medium shall be destroyed in a way that renders restoration of the information contained therein impossible.

§ 39. Adoption of Processing Procedure

- (1) The requirements for processing state secrets and classified media, including more specific INFOSEC requirements, except the requirements specified in subsection (2) of this section, shall be established by a

regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.

(2) The Minister of Defence shall adopt a regulation, specifying the following, for INFOSEC purposes:

- 1) requirements to encrypted materials and processing and protection thereof;
- 2) requirements for ensuring emission security;
- 3) requirements for computer and local network security.

(3) Parts of the regulation, specified in subsection (2) of this section, that contain state secrets, are classified, as provided by clause 10 2) of this Act. The regulation is submitted to the Surveillance Committee of Security Authorities of the Riigikogu for notification purposes.

Sub-Division 2

Admissibility to Process State Secrets

§ 40. Admissibility to Process State Secrets

(1) State secrets and classified media may be processed on an immovable or a movable possessed by a state agency or Eesti Pank.

(2) With the appropriate permit issued by the Security Police Board (hereinafter referred to as the 'processing permit'), state secrets and media containing thereof may also be processed outside an immovable or a movable possessed by a state agency or Eesti Pank, provided that the person has a justified need for that.

(3) Processing permit may be issued to:

- 1) a natural person;
- 2) a legal person in public law of Estonia;
- 3) a legal person in private law registered in Estonia;
- 4) a legal person of a foreign state for the participation of the person in negotiations concerning a public or international procurement or if the agency which

possesses state secrets needs to permit access by such person to the state secrets in connection with the functions imposed on the agency and if the person has the necessary special knowledge or skills to assist in the performance of such functions.

(4) Processing permits are granted to legal persons only after the person organising the protection of state secrets with the legal person has been issued a Personnel Security Clearance.

(5) Processing system may only be used for the processing of state secrets if a statement of accreditation or interim approval to operate, issued by the Information Board, is available.

§ 41. Application for Processing Permit or Extension of Term Thereof

(1) In order to obtain a processing permit or to be granted extension of the term thereof, a person shall submit an application to the Security Police Board through a constitutional institution, governmental authority or state agency administrated by a government authority (hereinafter the 'supporter of processing permit') which justifies the need for access and supports the receipt or extension of the term of the permit, to which the following documents shall be appended:

- 1) a letter from the supporter of processing permit, setting out the type or types of state secrets that the processing permit is applied for, together with reference to the basis of classification of such information and which justifies the need for processing state secrets and media containing thereof outside the immovable or a movable possessed by a state agency or Eesti Pank by the person who is in an employment, service, or contractual relationship or applying for such relationship and which supports the receipt of a processing permit or extension of the term thereof;
- 2) a document that proves access to state secrets or a verified copy thereof in the case of a natural person, except in cases specified in subsection (5) of this section or if right for access was granted by the Security Police Board;

- 3) documents specified in clauses 27 (1) 2) and 3) of this Act in the case of a legal person and a completed form of natural persons upon application for processing permit or, upon extension of the term of an processing, a completed annex to the form.
- (2) Upon extending the term of a processing permit, one may, if applicable, apply for access to state secrets with a classification level lower or higher than specified in the valid processing permit.
- (3) In order to be granted extension of the term of a processing permit, an application together with the documents appended thereto shall be submitted to the Security Police Board not later than three months before the expiry of the Personnel Security Clearance.
- (4) The term of a processing permit shall be extended until the decision to extend or to refuse from reviewing the application has been adopted in the case of the timely submission of documents required for granting an extension of the term of a processing permit.
- (5) The application specified in subsection (1) or (2) of this section may be submitted together with the application for the issue of a Personnel Security Clearance or the extension the term thereof.
- (6) The format of the application for a processing permit or extension of the term thereof and the format of an application form and the annex thereto shall be established by a regulation of the Government of the Republic, adopted under the procedure applicable to the protection of a state secret and the classified information of foreign states.

§ 42. Bases for Refusal to Issue Processing Permit or Extend Term Thereof

- (1) A processing permit shall not be issued to or an extension of the term thereof shall be refused for natural persons:
 - 1) who lack the right for access;
 - 2) who lack a justified need to process state secrets or classified media containing thereof outside an immovable or a movable possessed by a state agency;

- 3) who have not provided conditions required for the protection of state secrets and classified media, provided by this Act and legislation issued on the basis thereof;
- 4) who have been deprived of processing rights.

(2) A processing permit shall not be issued to or an extension of the term thereof shall be refused for legal persons:

- 1) who lack the need for access;
- 2) with respect to whom the circumstances specified in clauses (1), 2) – 4) of this section exist;
- 3) who do not meet the requirements, specified in subsections 40 (3) or (4) of this Act;
- 4) with respect to whom the circumstances specified clause 32, (1), 7), 8) or 10) of this Act exist;
- 5) with respect to whom the conditions serving as a pre-requisite for the initiation of bankruptcy proceedings exist or who are subject to initiation of liquidation procedure.

(3) Issue of a processing permit or extension of the term thereof may be refused for legal persons:

- 1) with respect to whom the circumstances specified in clauses 32 (2) 1) – 8), 10) or 11) of this Act exist;
- 2) whose commercial or trading activities are contrary to good practices and good morals;
- 3) who have, during the last three years, materially violated any public procurement contracts;
- 4) at least one third of share or participation of which belongs to a person that can not be identified.

(4) The procedure for checking the existence of circumstances specified in clause (1) 3) of this section shall be established by a regulation of the Government of the Republic, adopted under the procedure applicable to the protection of a state secret and classified information of foreign states.

(5) Security vetting shall be performed on the person under the provisions of this Act to ensure the circumstances specified in subsections (2) and (3) of this section.

(6) An agency, constitutional institution and legal body is required to notify the Security Police Board of persons in respect of whom the circumstances provided for in subsection (1), (2) or (3) of this section become evident.

§ 43. Issue of Processing Permit and Extension of Term Thereof

(1) The basis for issue of a processing permit or extension of the term thereof is a decision which is made on the basis of inspecting the circumstances specified in clause 42 (1) 3) of this Act and which shall be founded on all information gathered in the course of such checks.

(2) The basis for issue of a processing permit to legal persons or extension of the term thereof is also a decision which, in addition to the decision specified in subsection (1) of this section, is made on the basis of security vetting and which shall be founded on all information gathered in the course of security vetting.

(3) The issue of a processing permit or extension of the term thereof shall be decided not later than within two months in the case of natural persons and not later than within six months in the case of legal persons, after the submission of a valid application. In cases specified in subsection 41 (5) of this Act, the issue of a processing permit or extension of the term thereof shall be decided immediately after the issue of a Personnel Security Clearance or extension of the term thereof.

(4) The term described in the first sentence of subsection (3) of this section may be extended by three months in the case of a natural person and by six months in the case of a legal person in the following cases:

- 1) where it is necessary for the decision on the grant of a processing permit to be based on information originating from a foreign state;
- 2) where it has not been possible to conduct an interview with the legal person applicant or a representative of the applicant for a processing permit within six months in the course of security vetting due to material circumstances depending on the applicant;
- 3) where information gathered about the legal person applying for a processing permit in the course of security vetting indicates that bases for refusal to issue a Personnel Security Clearance are likely to become evident within the following six months;
- 4) where information gathered in the course of security vetting indicates that bases for refusal to issue a Personnel Security Clearance may cease to exist in respect of the legal

person applying for a processing permit and subject to security vetting within the following six months.

(5) The Security Police Board shall refuse to review the application in the following cases:

1) the granting of a processing permit or extension of the term thereof to state secrets classified at the same or lower level has been refused to this person earlier and the application does not show that the circumstances serving as the grounds for refusal have lapsed;

2) upon the request of the applicant of the processing permit or his/her supporter to refuse a review of the application;

3) where it has not been possible to conduct an interview with the legal person applicant for a processing permit in the course of security vetting within the period of six months as of the submission of required documents due to immaterial circumstances depending on the applicant or its representative;

4) in other situations provided by law.

(6) If a processing permit to the classification level of state secret specified in the application cannot be issued to a person or the extension of the term thereof is not possible as a result of the consideration of circumstances specified in subsection 42 (3) of this Act or checking of the conditions specified in clause 42 (1) 3) of this Act, but it would be possible to issue or extend the term of a processing permit to a lower level of classification, a Personnel Security Clearance is issued or extension of the term thereof is granted for a lower level of classification, if considered necessary by the applicant for the processing permit and his/her supporter.

(7) A processing permit is issued or the term thereof is extended for a fixed term, if the need to process state secrets and media containing thereof may also be processed outside an immovable or a movable possessed by a state agency or Eesti Pank is of a temporary nature; in the case of a natural person applicant, the term shall not extend the term of right for access to state secrets.

(8) A processing permit or extension of the term thereof shall be prepared on the letterhead with security features of the Security Police Board, with the signature of the Director General of the Security Police Board. A processing permit or a notice concerning extension of the term thereof shall set out the following data:

- 1) the date of issue of the processing permit or extension of the term thereof and the number of the permit;
- 2) the basis and justification for issue of the processing permit or extension of the term thereof;
- 3) the given name, surname, personal identification code and job or position of the person, if the processing permit is issued to a natural person;
- 4) name, seat and registry code of the person, if the processing permit is issued to a legal person;
- 5) the classification of state secrets which the person is permitted to process with a reference to the basis of classification;
- 6) the term of the processing permit.

(9) A notice concerning the issue of a processing permit or the extension of the term thereof shall be sent by the Security Police Board to the applicant through the supporter of processing permit within five working days as of the adoption of the decision.

(10) Upon refusal to issue a processing permit or to extend the term thereof, the Security Police Board shall send an officially certified copy of the decision to refuse to issue the permit or to extend the term thereof to the person who was denied the issue of a processing permit or extension of the term thereof and a notice regarding the decision is sent to the supporter of processing permit, within five working days as of the adoption of the decision.

§ 44. Expiry of Processing Permit

(1) A processing permit shall expire:

- 1) upon the expiry of a right for access to state secrets, granted to a natural person;
- 2) upon termination of a legal person;
- 3) upon revocation of the right for processing from a person with an enforced court judgment or the decision of a body conducting extrajudicial proceedings;
- 4) upon expiry of the term specified in a processing permit;
- 5) upon revocation of a processing permit.

(2) A processing permit shall be revoked if;

- 1) a person's justified need to process state secrets and media containing thereof may also be processed outside an immovable or a movable possessed by a state agency has ceased to exist;
- 2) the conditions provided by the person do not comply with the conditions required for the protection of state secrets and classified media, provided by this Act and legislation issued on the basis thereof;
- 3) the right for access to state secrets granted to a natural person has expired;
- 4) circumstances specified in subsection 42 (2) of this Act exist in the case of a legal person.

(3) In the case of a short-term lapse in the justified need to process state secrets and media containing thereof may also be processed outside an immovable or a movable possessed by a state agency, a processing permit need not be revoked.

(4) A processing permit issued to a legal person may be also revoked if:

- 1) circumstances specified in subsection 42 (3) of this Act exist with respect to the person;
- 2) the legal person is reorganised.

(5) A processing permit shall be revoked by the Director General of the Security Police Board. The Security Police Board shall send an officially certified copy of the decision to revoke the permit to the person whose processing permit was revoked and a notice regarding the decision to the supporter of processing permit within five working days as of the adoption of the decision.

(6) The supporter of processing permit and an agency, constitutional institution or a legal body, in which a natural person whose processing permit is revoked or identified as invalid, is employed or contracted by, shall promptly be notified of the revocation of the processing permit of the natural person.

(7) The supporter of processing permit and the head or directing body of the legal person whose processing permit is revoked or identified as invalid shall promptly be notified of the revocation of the processing permit of the legal person.

(8) The person who has been issued the processing permit must return all the classified media in his/her possession to the possessor of the classified information, which granted

him or her access to state secrets, upon the expiry of the processing permit. Media that only contain state secrets created by having held the processing permit must be handed over to the agency that initiated the creation of information and to the Security Police Board in all the other cases.

§ 45. Obligations of a Legal Person in Private Law Who Holds a Processing Permit

A legal person in private law who hold a permit for processing state secrets is, in addition to compliance with the requirements specified in § 19 of this Act, required to notify the Security Police Board promptly of the following circumstances:

- 1) a merger, division or transformation of a legal body;
- 2) the changing of members of the Management or Supervisory Board;
- 3) the contact details of the members of the Management or Supervisory Board if they are staying abroad for a period longer than three months;
- 4) a change in material liabilities if the incurring material liability is bigger than 30 percent of equity or if the total value of material liability exceeds 70 percent of equity;
- 5) bankruptcy or liquidation proceedings that have been initiated with respect to a legal person.

§ 46. Statement of Accreditation of a Processing System and Interim Approval to Operate

- (1) The Information Board shall issue a statement of accreditation to a processing system as a result of accreditation, provided that the processing system complies with INFOSEC requirements. The classification level of information that is permitted to be processed by the system and the term of the statement of accreditation shall be specified in the statement of accreditation.
- (2) The Information Board shall issue an interim approval to operate to a processing system as a result of accreditation, if the processing systems do not comply with INFOSEC requirements but the related security risks are, nevertheless, temporarily acceptable. The interim approval to operate shall specify the classification level of information that is permitted to be processed by the system, the term of the interim approval to operate, and

the obligation, conditions, and term for new accreditation of the processing system.

- (3) If electronic processing of state secrets takes place outside an immovable or a movable possessed by a state agency or Eesti Pank, the issue of a statement of accreditation or an interim approval to operate is, in addition to the compliance with the requirements specified in subsections (1) and (2) of this section, subject to the availability of a valid state secrets processing permit.
- (4) The procedure for the application for and revocation of a statement of accreditation to a processing system and interim approval to operate shall be established by a regulation of the Government of the Republic under the procedure applicable to the protection of a state secret and classified information of foreign states.

Division 4

Security Vetting

§ 47. Basis for Performing Security Vetting

- (1) The performance of security vetting shall only mean the checking of the existence of circumstances specified in § 32 and subsections 42 (2) and (3) of this Act and the proceedings performed must not restrict the fundamental rights and freedoms of persons more than necessary to establish the presence of respective grounds.
- (2) In order to obtain a right for access under a Personnel Security Clearance or to obtain access on the basis of an order of a investigative body or Prosecutor's Office or on the basis of a court ruling, or to obtain a processing permit of a legal person or to be granted extension of the term thereof, an applicant must pass security vetting.
- (3) The agency performing security vetting is also entitled to check for the existence of circumstances specified in § 32 and subsections 42 (2) and

(3) of this Act during the term of a Personnel Security Clearance and processing permit of a legal person.

(4) If there is a justified suspicion that circumstances providing the grounds for refusal of the issue of a Personnel Security Clearance may exist with respect to a person, security vetting may be performed with respect to the following persons, if requested by a head or managing body of an agency, specified in subsection 27 (2) or (5) of this Act:

- 1) a person who is about to be employed in a position which requires access to state secrets classified as 'restricted' or who is already holding such office;
- 2) who is considered to be given access to state secrets classified as 'restricted' or who has a right for access, granted under the procedure specified in subsection 27 (5) of this Act.

(5) In cases specified in subsection (4) of this section, the head or managing body of an appropriate agency (hereinafter referred to as 'applicant') is required to submit a justified application to an agency competent to perform security vetting who shall then adopt a decision regarding their performance of security vetting within two weeks as of the receipt of such an application and shall notify the agency that submitted the application.

(6) Security vetting may only be performed if a person has given their consent specified in clause 27 (19) 3) of this Act.

§ 48. Security Vetting Authorities

(1) Security vetting shall be performed by the Security Police Board, except in the cases specified in subsections (2) and (3) of this section.

(2) The General Staff of the Defence Forces shall perform security vetting in:

- 1) the Defence Forces and the Defence League, except in respect to the Commander of the Defence Forces and Chief of Staff of the General Staff of the Defence Forces and his deputy and

- 2) the Ministry of Defence with regard to members of the Defence Forces in contractual active service (except the Permanent Undersecretary and Deputy Undersecretary) and in agencies within the area of government of the Ministry of Defence.
- (3) The Information Board shall perform security vetting with regard to the following persons:
 - 1) those who stand as candidates for the position of security officials at the Information Board and persons who are in the service of the Information Board, except the Director General of the Information Board and his/her deputy;
 - 2) the Director General of the Security Police Board and his/her deputy;
 - 3) the Permanent Undersecretary and Deputy Undersecretary of the Ministry of Internal Affairs;
 - 4) Public Prosecutors.

§ 49. Performance of Security Vetting

- (1) Security vetting shall be performed by the General Staff of the Defence Forces pursuant to the procedure provided for in the Surveillance Act and in the Security Authorities Act, considering the specificities of this Act.
- (2) A committee, consisting of at least three members, is formed at a security authority by a relevant Minister or the Commander of the Defence Forces in the General Staff of the Defence Forces at the proposal of an agency performing security vetting or by a head of a structural unit of the Defence Forces, respectively, which deals with intelligence and counter-intelligence for the purpose of reviewing the information collected as a result of security vetting.
- (3) The committee, specified in subsection (2) of this section, shall make proposals to a person or a body who is competent to grant a right for access; issue a Personnel Security Clearance or processing permit or extend the term thereof; adopt decisions concerning the revocation of a right for access or access or processing permit; adopt decisions concerning the issue of a right for access, Personnel Security Clearance or processing permit; or adopt decisions concerning

the extension of the term thereof on the basis of information collected as a result of security vetting.

- (4) For the purposes of security vetting, an agency performing security vetting shall conduct an interview with a person subject to security vetting or, in the case of a legal person, his/her legitimate representative (hereinafter referred to as 'applicant'). If security vetting is performed to adopt a decision concerning extension of the term of right for access, access or processing permit, the agency performing security vetting shall only conduct an interview, if applicable. An agency performing security vetting shall record the interview.
- (5) A person interviewed is questioned regarding the circumstances specified in § 32 and subsections 42 (2) and (3) of this Act. The applicant shall be entitled to give explanations considered important for checking the existence of the aforementioned circumstances.
- (6) An agency conducting security vetting shall finish the performance of security vetting immediately at the request of the checked person, head of an agency specified in subsections 27 (2) and (5) of this Act, and an agency supporting the issue of an access or processing permit. If this is the case, the person will be refused the granting of a right for access or the issue of a processing permit or extension of the term thereof or will be deprived of the right for access to state secrets classified as 'restricted' or the issued access or the processing permit will be revoked.
- (7) If a suspicion that a person may suffer from mental illness, mental disability or some other psychic disorder which may limit his/her ability to interpret his/her behaviour or to control it incurs upon the conduct of security vetting, an agency performing security vetting shall ask this person for consent to be sent for a psychiatric examination. Should the person refuse to give consent, he or she will be refused the granting of a right for access or the issue of a processing permit or extension of the term thereof or will be deprived of the right for access to state secrets classified as 'restricted' or the issued access or processing permit will be revoked.

- (8) The procedure for psychiatric examination to be performed during security vetting and the form of conclusion shall be established by a regulation of the Minister of Social Affairs.

Chapter 3

CLASSIFIED INFORMATION OF FOREIGN STATES

§ 50. General Provisions

- (1) If not provided otherwise by an international agreement, the provisions applicable to the appropriate level of classification of state secrets, provided in Chapter 1, Chapter 2 Division 3 and Chapter 4 are also applicable to the classified information of foreign states, considering the specificities detailed in this Chapter.
- (2) If the conformity of the classification level of classified information of foreign states and state secrets has not been determined by an international agreement, the conformity of such levels shall be determined by the national security authority on the basis of the conformity of protective measures.
- (3) International agreements shall serve as the basis for determining the term of classification of classified information of foreign states and media containing thereof. If the originator of information of foreign states has not specified the term of classification for such information, the classification of the medium may only be declassified at the permission of the originator of classified information of foreign states.
- (4) Information processed as classified information of foreign states with no legal grounds is declassified or the level, legal grounds or term of classified information of foreign states classified at an incorrect level, wrong legal grounds or wrong term of a state secret is changed, as provided in § 15 of this Act, if the originator of classified information of foreign states has previously granted his/her consent. Should the identification of the originator of the classified information of foreign states be impossible or if the originator of the information has ceased to exist, the national security authority shall declassify the classification of classified information of foreign states processed as a state secret

with no legal grounds or shall change the level, grounds or term of classified information of foreign states classified at an incorrect level, wrong legal grounds or wrong term of classified information of foreign states.

- (5) If provided by an international agreement, the medium containing classified information of foreign states shall be marked with a marking given by the originator of classified information of foreign states and classification marking of the conforming level of classification of a state secret.
- (6) If requirements established for a processing system, used for processing classified information of foreign states, provided under an international agreement, are stricter than the requirements established for a processing system by this Act or legislation issued hereunder, the processing system, used for processing classified information of foreign states must be additionally accredited, as provided by § 46 of this Act.
- (7) Regulations adopted by the Government of the Republic under subsections 20 (4), 27 (13), 31 (5), 36 (3), 39 (1), 41 (6), 42 (4) and 46 (4) of this Act, may establish specificities to be observed for the purpose of the protection of classified information of foreign states.
- (8) Specifications for the protection of classified information of foreign states may be established by regulations of the Minister of Defence as provided in subsection 39 (2) of this Act.

§ 51. Access to Classified Information of Foreign States

- (1) If not provided otherwise by an international agreement, the provisions provided in Chapter 1, Chapter 2 Division 3 and Chapter 4 are also applicable to giving access to the classified information of foreign states, considering the specificities detailed in this Chapter.
- (2) If the grounds for refusing right for access, provided in an international agreement, are stricter than the grounds stipulated in subsections 32 (1) and (2) or subsections 42 (2) – (3) of this Act, the existence of circumstances arising from an international agreement is also checked when security vetting is performed and the existence of the appropriate circumstance shall serve as the grounds for refusing right for access

to classified information of foreign states. If the originator of classified information of foreign states prohibits granting of right for access to a person, such a person is not granted right for access to respective classified information of foreign states.

- (3) If an international agreement requires performing of security vetting for giving right for access to classified information of foreign states, such security vetting shall be performed with respect to persons holding the right for access by virtue of office, except the President of the Republic.
- (4) If the issue of a Personnel Security Clearance Certificate for Access to Foreign Classified Information is specified in an international agreement as a pre-requisite for granting right for access to classified information of foreign states of the respective level, a certificate granting access to classified information of foreign states (hereinafter referred to as ‘Personnel Security Clearance Certificate for Access to Foreign Classified Information’) is issued to give access to classified information of foreign states. National security authority shall issue the Personnel Security Clearance Certificate to Foreign Classified Information.
- (5) National security authority shall immediately notify an agency performing security vetting with respect to a person of the issue of a Personnel Security Clearance Certificate for Access to Foreign Classified Information to a natural or legal person, revocation or identification of invalidity of such a certificate.
- (6) Specific procedure for the issue, refuse to issue, extension of the term and revocation of a Personnel Security Clearance Certificate for Access to Foreign Classified Information is established with the Regulation of the Government of the Republic, adopted under the procedure applicable to the protection of a state secret and classified information of foreign states.

§ 52. Competence of National Security Authority for Organisation of Protection of Classified Information of Foreign States

- (1) national security authority has the following functions under this Act, legislation issued on the basis thereof and with international agreements:
 - 1) receipt of classified information of foreign states from the originator thereof, processing of and organising access to such information, maintaining records

concerning classified information of foreign states and the agencies, constitutional institutions, natural and legal persons who possess such information;

- 2) supervision over the security measures applied by agencies, institutions, natural and legal persons for the protection of classified information of foreign states and access of their employees to such information, including at the representations of Estonia and in the units of the Defence Forces which are outside the territory of the Republic of Estonia;
- 3) in the case of the unlawful disclosure of classified information of a foreign state, informing the originator of the information of the circumstances of the disclosure, under the conditions prescribed by the international agreement;
- 4) issue of Personnel Security Clearance Certificates for Access to Foreign Classified Information and informing the originator of the information of the circumstances of the granting of access, under the conditions prescribed by the international agreement;
- 5) notification of possessors of classified information of foreign states of changing the grounds, level and term of classification of classified information of a foreign state;
- 6) provision of periodic training in order to guarantee the conformity of the security measures with the requirements set for the protection of classified information;
- 7) making proposals to the Security Committee of the Government of the Republic for the elimination of omissions and avoidance of violations for the purpose of protection of classified information of a foreign state;
- 8) performance of other duties imposed thereon by international agreements.

(2) For performance of the functions provided in subsection (1) of this section, national security authority has the right to:

- 1) examine, in the process of supervision operations, all the necessary information;
- 2) obtain, pursuant to the Administrative Co-operation Act, professional assistance from security authorities and the General Staff of the Defence Forces within the limits of their competence;
- 3) issue precepts to possessors of classified information of a foreign state for the elimination of a violation or danger of a violation of requirements arising from international agreements or this Act;

- 4) issue precepts to possessors of classified information of a foreign state to suspend the processing of classified information of foreign states or to take the media containing classified information temporarily into storage until establishment of the required conditions, if a violation or danger of requirements arising from international agreements or this Act or legislation issued on the basis thereof that may result in disclosure of classified information has been established as the result of checks.
- (3) If not provided otherwise by an international agreement, national security authority shall not organise or check the information exchange of security authorities and Central Criminal Police, conducted under the provisions specified in subsections 35 (4) and (5) of this Act.
- (4) Should national security authority impose a penalty payment for the failure to comply with the precept, specified in clauses (2) 3) and 4) of this section, the maximum value of such penalty payment shall be 50,000 kroons.
- (5) Upon the termination of activities of an agency, institution or legal person in possession of classified information of a foreign state, or on demand of national security authority, the media containing classified information shall be immediately transferred to national security authority.
- (6) National security authority officials are entitled to carry a service weapon and use it upon the fulfilment of their duties pursuant to the procedure provided for in this Act.
- (7) The Minister of Defence prescribes the types of service weapons which national security authority officials are entitled to use and the procedure for handling these weapons by a regulation.

Chapter 4

LIABILITY

§ 53. Liability for the Violation of this Act

- (1) Violation of requirements to protection of state secrets by a person holding the right for access of state secrets, if accompanied by danger of disclosure or

becoming known to a person with no right of access, processing of information as state secrets with no legal grounds, classification of state secret on wrong legal grounds, at an incorrect level or for a wrong term, failure to classify a state secret, failure to declassify a state secret after the lapse of a threat to security before the expiry of classification term or failure to comply with the notification requirement, specified in clauses 19 3), 4), 6) and 7), subsection 32 (4), subsection 42 (6) or § 45 of this Act, shall be punishable by a fine of up to 200 fine units or detention.

- (2) Conduct specified in subsection (1) of this section, if the object of a misdemeanour is a state secret classified as 'secret' or top secret', shall be punishable by a fine of up to 300 fine units or detention.
- (3) Disclosure, illegal communication or granting of illegal access to state secrets by a person, required to safeguard a state secret, if the conduct was due to negligence, and also the loss of classified media, shall be punishable by a fine of up to 300 fine units or detention.
- (4) Conduct specified in subsection (1) – (3) of this section, if committed by a legal person, shall be punishable by a fine of up to 500, 000 kroons.
- (5) A person shall not be relieved from responsibility when committing a misdemeanour, the object of which was a state secret, information was declassified or the legal grounds, classification level or term for classification of such information was changed, except if there were no legal grounds for the classification of such information. A person shall be responsible for classification of information with no legal grounds also after the declassification of such information.
- (6) Provisions of the General Part of the Penal Code and Code of Misdemeanour Procedure shall be applicable to the misdemeanour, specified in this Article.
- (7) If a person is deprived from a right for access to a state secret or the right for processing state secrets and classified information of a foreign state outside an immovable or a movable possessed by a state agency or Eesti Pank for commitment of a misdemeanour under the State Secrets and Classified

Information of Foreign States Act or legislation issued on the basis thereof, such a person must apply again for the respective right for access or processing permit to obtain right for access or processing right.

- (8) Extrajudicial proceedings in a misdemeanour specified in this Article shall be conducted by the Security Police Board.

Chapter 5

IMPLEMENTING PROVISIONS

§ 56. Review of Media

- (1) A possessor of classified information is required to review the classified media within one year as of the enforcement of this Act, except media specified in subsection (2) of this section.
- (2) Medium kept in an archive of a possessor of classified information shall review the proceedings for the processing of classified media, except the storage requirements, as necessary.
- (3) All the media, specified in subsection (2) of this section, must be reviewed, regardless of their processing needs, no later than within three years as of the enforcement of this Act.
- (4) If information contained by a medium is not classified information for the purposes of this Act, such information is declassified and the medium is marked, as provided by this Act. If information contained by a medium is classified at a different level, legal grounds if different for the purposes of this Act, the classification marking of a medium, marking concerning the grounds of classification, or term of classification shall be respectively changed.
- (5) Section 15 or subsection 50 (4) of this Act shall apply as the grounds for considering declassification of information and changing the level, legal grounds or term of classification.

§ 57. Validity of Right for Access Granted Prior and Performance of Security Vetting

- (1) Personnel Security Clearances, Personnel Security Clearance Certificate for Access to Foreign Classified Information, temporary permits of use of processing systems and statements of accreditation, issued before the enforcement of this Act, shall remain valid until the expiry specified in such documents.
- (2) An open-ended right for access, granted under subsection 23 (3) of the State Secrets Act (RT I 1999, 16, 271; 2005, 64, 482) shall remain in force for the period of one year as of the enforcement of this Act, if the person is not deprived of the right for access prior to this time.
- (3) Security vetting may be performed with respect to a person, having been issued a Personnel Security Clearance, Personnel Security Clearance Certificate for Access to Foreign Classified Information or holding right for access before the enforcement of this Act under subsection 23 (2) or (3) of the State Secrets Act (RT I 1999, 16, 271; 2005, 64, 482) as provided in the State Secrets Act (RT I 1999, 16, 271; 2005, 64, 482) and this Act until the expiry of such right for access or granting of right for access under this Act.

§ 58. Access to State Secrets After the Establishment of List of Positions

- (1) A person who is employed in a position where, after establishment of the list of positions specified in subsection 20 (5) of this Act, he/she must have the right of access to state secrets classified as "restricted" but who do not hold a valid Personnel Security Clearance, shall submit the documents specified in clause 27 (10) 2) and 3) to the agency which performs security vetting not later than within one month after the entry into force of the aforementioned list of positions.
- (2) A person who is employed in a position where, after establishment of the list of positions specified in subsection 20 (5) of this Act, he/she must have the right of access to state secrets classified as "confidential" or higher but who does not hold a valid Personnel Security Clearance granting right for access to state secrets of respective level, shall submit a Personnel Security Clearance application for performing security vetting with respect to that person to the agency which performs security vetting not later than within one month after the entry into force of the aforementioned list of positions.

§ 59. Amendment of Databases Act

The Databases Act (RT I 1997, 28, 423; 2004, 30, 204) shall be amended as follows:

- 1) in subsection 3 (4), the words ‘State Secrets Act (RT I 1994, 45, 720; 1996, 42, 809)’ shall be replaced with the words ‘State Secrets and Classified Information of a Foreign States Act’;
- 2) the words ‘or classified information of a foreign state’ are added to subsection 11¹ (1) after the words ‘state secret’;
- 3) the words ‘state secret’ shall be replaced with the words ‘state secrets and classified information of a foreign state’ in the appropriate case in clause 26 (2) 11), 40 (1) 7), 47 (1) 7).

§ 60. Amendment of Archives Act

Section 42 (1) of the Archives Act (RT I 1998, 36/37, 552; 2004, 28, 188) shall be amended and worded as follows:

‘(1) The procedure for access to records containing a state secret and classified information of a foreign state is provided for in the State Secrets and Classified Information of Foreign States Act and legislation issued on the basis thereof.’

- 1) the words ‘or classified information of a foreign state’ are added clause § 2 (2) 1) after the words ‘state secret’.

§ 61. Amendment of Public Information Act

The Public Information Act (RT I 2000, 92, 597; 2005, 39, 308) shall be amended as follows:

- 1) the words ‘or as classified information of a foreign state’ are added to clause 2 (2) 1) after the words ‘as a state secret’;
- 2) the words ‘if the information does not constitute a state secret or classified information of a foreign state’ shall be added to clause 35 (1) 3) after the words ‘foreign relations of the state’;
- 3) the words ‘or classified information of a foreign state’ are added to clause 35 (1) 4) after the words ‘state secret’;

4) clauses 12) and 13) are added to subsection 35 (1), worded as follows:

'12) information concerning the state assets to be transferred into the possession of the Defence forces for improving operational readiness and upon conduct of mobilisation, if the information does not constitute a state secret or classified information of a foreign state;

13) information concerning national defence duty, if the information does not constitute a state secret or classified information of a foreign state.'

§ 62. Amendment of Public Service Act

The Public Service Act (RT I 1995, 16, 228; 2006, 26, 193) shall be amended as follows:

- a. the words 'or classified information of a foreign state' are added to subsection 14 (3) after the words 'state secret';
- b. Article 39¹ is repealed;
- c. clause 117 (1) 7) shall be amended as follows:

'7) If a person holds an office where access to state secrets is a prerequisite for employment and circumstances specified in subsection 32 (1) of the State Secrets and Classified Information of Foreign States Act is existing with respect to that person or the person has been denied the right for access to the classification level of state secrets or classified information of a foreign state, required of that position, under the provisions of the State Secrets and Classified Information of Foreign States Act or the person has been deprived of right for access to the classification level of state secrets or classified information of a foreign state, required of that position.'

§ 63. Amendment of Eesti Pank Act

The Eesti Pank Act (RT I 1993, 28, 498; 2006, 29, 219) shall be amended as follows:

- 1) Section 11¹ shall be amended and worded as follows:

§ 11¹. Access of the Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank to State Secrets and Classified Information of a Foreign State

- (1) The Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging their functions.
- (2) If, under an international agreement, performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to the Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank, except a member of the Riigikogu, being a member of the Executive Board of Eesti Pank.
- (3) Security vetting with respect to the Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank shall be performed by the Security Police Board as provided by the State Secrets and Classified Information of Foreign States Act.
- (4) For passing security vetting, the Governor of Eesti Pank, Chairman or member of the Executive Board of Eesti Pank is required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the Security Police Board.
- (5) The Security Police Board shall perform security vetting with respect to the Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank within three months as of the receipt of documents, specified in subsection (4) of this section. A Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under

the procedure specified in the State Secrets and Classified Information of Foreign States Act.’;

2) Subsection 11² (1) shall be amended and worded as follows:

‘(1) Candidates for the position of the Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank must pass security vetting before being appointed as the Governor of Eesti Pank, Chairman or member of the Executive Board of Eesti Pank, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.’;

3) the words ‘in the Surveillance Act (RT I 1994, 16, 290; 1995, 15, 173; 1996, 49, 955; 1997, 81, 1361; 93, 1557; 1998, 47, 698; 50, 753; 51, 756; 61, 981; 98/99, 1575; 101, 1663; 1999, 16, 271; 31, 425; 95, 845; 2000, 35, 222; 40, 251; 102, 671; 2001, 3, 9; 7, 17)’ in § 11² (3) shall be replaced with the words ‘in the Security Authorities Act’;

4) the words ‘top secret’ level’ in subsection 11² (4) shall be replaced with the words ‘at ‘top secret’ level’;

5) the words ‘committee for protection of state secrets’ in subsection 11² (6) shall be replaced with the words ‘Security Committee of the Government of the Republic’ and the words ‘in subsection 30 (2¹) of the State Secrets Act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387) shall be replaced with the words ‘In subsection 33(4) of the State Secrets and Classified Information of Foreign States Act’;

6) subsection (7) shall be added to § 11², worded as follows:

‘(7) A candidate may be appointed for office, supported by data collected as the result of security vetting, within nine months as of the communication of information collected as the result of security vetting to a competent authority or constitutional institution by an agency performing security vetting. A candidate may be appointed to the office after the expiry of this term only after passing another security vetting.’

§ 64. Amendment of Republic of Estonia Employment Contracts Act

Clause 4), worded as follows, shall be added to subsection 101 (1) of the Republic of Estonia Employment Contracts Act (RT 1992, 15/16, 241; 2006, 10, 64):

‘4) If a person holds an office where access to state secrets is a prerequisite for employment and circumstances specified in subsection 32 (1) of the State Secrets and Classified Information of Foreign States Act are existing with respect to that person or the person has been denied the right for access to the classification level of state secrets or classified information of a foreign state, required of that position, under the provisions of the State Secrets and Classified Information of Foreign States Act or the person has been deprived of right for access to the classification level of state secrets or classified information of a foreign state, required of that position.’

§ 65. Amendment of Building Act

The Building Act (RT I 2002, 47, 297; 2006, 43, 326) shall be amended as follows:

- 1) the words ‘or classified information of a foreign state’ are added to clause 23 (6) 2) and subsection(11) after the words ‘state secret’;
- 2) the words ‘information classified as state secret’ shall be replaced with the words ‘state secrets or classified information of a foreign state’ in clauses 29 (1), 5) and 6) and (2) 3);
- 3) the words ‘or classified information of a foreign state’ are added to clause 30 (4) 7) and subsection 32 (2) after the words ‘state secret’.

§ 66. Amendment of Electronic Communication Act

The words ‘classified information of a foreign state’ are inserted after the words ‘state secret’ in subsection 148 (5) of the Electronic Communication Act (RT I 2004, 87, 593; 2005, 71, 545).

§ 67. Amendment of Administrative Procedure Act

The words ‘classified information of a foreign state and’ are inserted after the word ‘secret’ in subsection 7 (3) of the Administrative Procedure Act (RT I 2001, 58, 354; 2005, 39, 308).

§ 68. Amendment of Personal Data Protection Act

The words ‘or classified information of a foreign state’ are inserted after the words ‘state secret’ in subsection 2 (2) of the Personal Data Protection Act (RT 2003, 26, 158; 2004, 30, 208).

§ 69. Amendment of Security Authorities Act

The Security Authorities Act (RT I 2001, 7, 17; 2006, 48, 357) shall be amended as follows:

- a. in clause 6 2), the following sentence fragment ‘protection, as provided by State Secrets Act (RT I 1999, 16, 271; 82, 752)’ shall be replaced with the words ‘and protection of classified information of a foreign state, as provided in the State Secrets and Classified Information of a Foreign States Act’;
- b. in subsection 7 (3), the words ‘right for access to state secret classified as ‘top secret’’ shall be replaced with the words ‘permit for processing state secret classified as ‘top secret’’;
- c. the words ‘classified information of a foreign state’ are inserted after the words ‘state secret’ in the first sentence of subsection 20 (2);
- d. the words ‘classified information of a foreign state’ are inserted after the words ‘state secret’ in the second sentence of subsection 20 (2);
- e. the first sentence of § 33 shall be amended and worded as follows:
‘Methods and devices to be used for the organisation and checking of special communication shall be established with the regulation of the Minister of Defence.’;
- f. Section 34 is repealed;
- g. the words ‘and classified information of a foreign state’ are inserted after the words ‘state secret’ in the second sentence of subsection 36 (7);
- h. Section 37 is repealed.

§ 70. Amendment of Surveillance Act

The Surveillance Act (RT I 1994, 16, 290; 2005, 39, 307) shall be amended as follows:

1) Clause 9 (1) 6) shall be amended and worded as follows:

‘6) need to perform security vetting, provided by law’;

2) Clause 9 (1) 6¹) is repealed;

3) Subsection 16¹ (4) shall be amended and worded as follows:

‘(4) Surveillance files that contain state secrets or classified information of a foreign state shall be stored and destroyed as provided by the State Secrets and Classified Information of Foreign States Act.’;

4) the words ‘state secrets’ shall be replaced with the words ‘state secrets, classified information of a foreign state’ in clause 17 (2) 3).

§ 71. Amendment of Defence Forces Services Act

The Defence Forces Services Act (RT I 2000, 28, 167; 2006, 53, 398) shall be amended as follows:

a. the words ‘committee for protection of state secrets’ shall be replaced with the words ‘Security Committee of the Government of the Republic’ in the appropriate cases throughout the Act;

b. Subsection 97¹ (1) shall be amended and worded as follows:

‘(1) Candidates for the position of the Commander of the Defence Forces must pass security vetting before being appointed, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.’;

c. the words ‘in the Surveillance Act (RT I 1994, 16, 290; 1995, 15, 173; 1996, 49, 955; 1997, 81, 1361; 93, 1557; 1998, 47, 698; 50, 753; 51, 756; 61, 981; 98/99, 1575; 101, 1663; 1999, 16, 271; 31, 425; 95, 845; 2000, 35,

222; 40, 251; 102, 671; 2001, 3, 9; 7, 17)' in § 97¹ (3) shall be replaced with the words 'in the Security Authorities Act';

(4) the words "top secret' level' in subsection 97¹ (4) shall be replaced with the words 'at 'top secret' level';

(5) in subsection 97¹ (5) the words 'with collected information' are added after the word 'those'; the words 'the Minister of Defence, communicating the collected information' are omitted and the words 'as of their receipt' shall be replaced with the words 'as of the verification of the results of security vetting';

(6) the words 'in subsection 30 (2¹) of the State Secrets Act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387) shall be replaced with the words 'in § 33 (4) of the State Secrets and Classified Information of Foreign States Act';

7) subsection (7) shall be added to § 97¹ and worded as follows:

'(7) A candidate may be appointed for office, supported by data collected as the result of security vetting, within nine months as of the communication of information collected as the result of security vetting to a competent authority or constitutional institution by an agency performing security vetting. A candidate may be appointed to the office after the expiry of this term only after passing another security vetting.'

8) Section 97² shall be amended and worded as follows:

'Only a person holding a valid Personnel Security Clearance classified as 'top secret' or holding an office, when becoming the Commander-in-Chief or Commander of the Defence Forces, that grants access to all the classification levels of state secrets by virtue of office, may be appointed as the Commander-in-Chief or Commander of the Defence Forces.';

9) Section 97³ shall be added, worded as follows:

§ 97³. Access of the Commander-in-Chief of the Defence Forces and Commander of the Defence Forces to State Secrets and Classified Information of a Foreign State

- (1) The Commander-in-Chief of the Defence Forces and Commander of the Defence Forces shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging their functions.
- (2) If, under an international agreement, the performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to the Commander-in-Chief of the Defence Forces and Commander of the Defence Forces.
- (3) For passing security vetting the Commander-in-Chief of the Defence Forces or Commander of the Defence Forces are required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the Security Police Board.
- (4) Security vetting with respect to the Commander-in-Chief of the Defence Forces and Commander of the Defence Forces shall be performed by the authority appointed by the Minister of Defence who shall communicate the documents, specified in subsection (3) of this section, to the agency performing security vetting.
- (5) The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to the Commander-in-Chief of the Defence Forces and Commander of the Defence Forces, to the Minister of Defence within three months as of the receipt of documents, specified in subsection (3) of this section for deciding whether the Commander-in-Chief of the Defence Forces and Commander of the Defence Forces have passed security vetting. An Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under the procedure specified in the State Secrets and Classified Information of Foreign States Act.;

10) The words ‘classified information of a foreign state’ are inserted after the words ‘state secret’ in the first sentence of clause 107¹ (1) 2);

11) The words ‘or classified information of a foreign state’ are inserted after the words ‘state secret’ in the first sentence of subsection 118 (4);

12) Section 154 (7) is repealed;

13) subsection 180 (2) shall be amended and worded as follows:

‘(2) The procedure for the protection of state secrets and classified information of a foreign state shall be established with the State Secrets and Classified Information of Foreign States Act.’

§ 72. Amendment of the Punishment Register Act

The Punishment Register Act RT I 1997, 87, 1467; 2006, 29, 224) shall be amended as follows:

a. the words ‘and checking of circumstances specified in clause 22 (1) 2²) of this Act’ are added after the word ‘performance’ in subsection 3¹ (2);

b. the words ‘or performance of security vetting’ are added to the end of clause 17 (1) 10);

c. clause 2², worded as follows, shall be added to 22 (1):

‘2²) security authorities, General Staff of the Defence Forces and security authorities’ supervision committee of the Riigikogu for checking the circumstances, specified in clause 32 (1) 8) and (2) 5) and 8) of the State Secrets and Classified Information of Foreign States Act.’;

d. Clause 22 (2) 1) shall be amended and worded as follows:

‘1) information specified in subsection 17 (2) of this Act, if the applicant is a person or an agency, specified in clauses (1) 1), 2), 2²) and 2³) of this section.’

§ 73. Amendment of the Penal Code

The Penal Code (RT I 2001, 61, 364; 2006, 46, 333) as amended as follows:

1) in subsection 47 (3), the words ‘or a misdemeanour relating to a state secret or classified information of a foreign state’ are added after the words ‘a misdemeanour relating to competition’;

2) Section 52¹ shall be added, worded as follows:

‘§ 52¹. Deprivation of a Right for Access to State Secret and Classified Information of a Foreign State and Right to Process State Secret and Classified Information of a Foreign State

(1) Additional punishment, consisting of deprivation of right for access to state secrets and classified information of a foreign state or deprivation of right to process state secrets and classified information of a foreign state immovable or a movable possessed by a state agency or Eesti Pank or deprivation of both rights may be imposed on a natural person offender for the violation of the State Secrets and Classified Information of Foreign States Act for the period of three years by court ruling or the decision of a body conducting extrajudicial proceedings.

(2) An additional punishment, consisting of deprivation of right to process state secrets and classified information of a foreign state immovable or a movable possessed by a state agency or Eesti Pank or deprivation of both rights may be imposed on a natural person offender for the violation of the State Secrets and Classified Information of Foreign States Act for a period of three years by court ruling or the decision of a body conducting extrajudicial proceedings.’;

3) the words ‘classified information of a foreign state’ are inserted after the words ‘state secret’ in the first sentence of subsection 271 (2);

4) Title 1 with the following wording shall be added to Chapter 15, changing the numeration of the following titles, as necessary:

Division 1

General Provisions

§ 230¹. Punishment for Offences Specified in this Chapter

A person shall not be relieved from responsibility when committing an offence, the object of which was a state secret, information was declassified, or the legal grounds, classification level or term for classification of such information was changed, except if there were no legal grounds for the classification of such information.’;

5) in §§ 232 and 234, the words ‘information classified as state secret or classified information of a foreign state or international organisation, communicated to Estonia under an international agreement’ are replaced with the words ‘state secret or classified information of a foreign state’;

6) Section 241 shall be amended and worded as follows:

‘§ 241. Disclosure of State Secrets and Classified Information of a Foreign State

- a. Disclosure, illegal communication or granting of illegal access to state secrets by a person, required to safeguard a state secret, if the conduct was due to negligence, and also losing of classified media, if the necessary elements of a crime are missing, is punishable by a pecuniary punishment or up to 5 years’ imprisonment.
- b. The same act, if committed by a legal person, is punishable by a pecuniary punishment.’;

7) Section 242 shall be amended and worded as follows:

‘§ 242. Disclosure of State Secrets and Classified Information of a Foreign State Through Negligence

- (4) Disclosure, illegal communication, or granting of illegal access to state secrets by a person, required to safeguard a state secret, if the conduct was due to negligence, and also the loss of classified media containing state secrets or classified information of foreign states, if:
 - 1) this causes considerable damage to the security of the Republic of Estonia, a foreign state, an international organisation or an institution established under an international agreement; or

2) the object of an offence was a state secret classified as ‘secret’ or ‘top secret’ or classified information of a foreign state,

is punishable by a pecuniary punishment or up to one year of imprisonment.

c. The same act, if committed by a legal person, is punishable by a pecuniary punishment.

8) Section 316¹ with the following wording shall be added to the Act:

‘§ 316. Classification of Information with no Legal Grounds and Classification of State Secret or Classified Information of a Foreign State at Wrong Legal Grounds, Wrong Classification Level or Term

(1) The classification of information with no legal grounds or the classification of a state secret or classified information of a foreign state at the incorrect legal grounds, level or for an incorrect term with the purpose of preventing the existence of an act classified as a criminal offence or its absence or identification or other circumstances of subject of proof is punishable by a pecuniary punishment or from one to five years’ imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment.

(3) A person shall not be relieved from responsibility when committing an offence, specified in this Article, if the information was declassified or the legal grounds, classification level or term for classification of such information was changed after the commitment of such offence.’

§ 74. Amendment of Courts Act

The Courts Act (RT I 2002, 64, 390; 2006, 48, 357) shall be amended as follows:

1) Section 8¹ with the following wording shall be added to the Act:

‘§ 8¹. Access of a Judge to State Secrets and Classified Information of a Foreign State

- (1) Judges shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging their functions.
- (2) If, under an international agreement, performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to a judge.
- (3) For passing security vetting, judges are required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the Supreme Court en banc.
- (4) The Supreme Court en banc shall appoint an authority performing security vetting that shall be communicated the documents, specified in subsection (3) of this section.
- (5) The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to a judge within three months as of the receipt of documents, specified in subsection (3) of this section to the Supreme Court en banc for deciding whether a judge has passed security vetting. A Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under the procedure specified in the State Secrets and Classified Information of Foreign States Act.;

2) Subsections 54 (2) and (3) are replaced with subsections (2) to (7) as follows:

‘ (2) Candidates for the position of a judge must pass security vetting before being appointed as a judge, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.

(3) For passing security vetting judges are required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the Security Police Board through Judges' Examination Committee.

(4) Security vetting of an applicant for the position of a judge shall be performed by the Security Police Board as provided by the Security Authorities Act.

(5) Information collected as a result of security vetting and related opinion is communicated by the Security Police Board to the Judges' Examination Committee within three months as of the receipt of the documents, specified in subsection (3) of this section.

(6) A candidate may be appointed for office, supported by data collected as the result of security vetting, within nine months as of the communication of information collected as the result of security vetting to a competent authority or constitutional institution by an agency performing security vetting. A candidate may be appointed to the office after the expiry of this term only after passing another security vetting.

(7) The Judges' Examination Committee shall communicate its opinion and documents, specified in subsection (3) and (5) of this section to the Supreme Court en banc and notify the examinee of the adopted decision.?

3) Subsection 52¹ (1) shall be amended and worded as follows:

‘(1) Candidates for the position of Chief Justice of a Supreme Court must pass security vetting before being appointed, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.’;

4) the words ‘in the Surveillance Act (RT I 1994, 16, 290; 1995, 15, 173; 1996, 49, 955; 1997, 81, 1361; 93, 1557; 1998, 47, 698; 50, 753; 51, 756; 61, 981; 98/99, 1575; 101, 1663; 1999, 16, 271; 31, 425; 95, 845; 2000, 35, 222; 40,

251; 102, 671; 2001, 3, 9; 7, 17)' in § 54¹ (4) shall be replaced with the words 'in the Security Authorities Act';

5) the words "top secret' level' in subsection 54¹ (4) shall be replaced with the words 'at 'top secret' level';

6) the words 'committee for protection of state secrets' in subsection 54¹ (6) shall be replaced with the words 'Security Committee of the Government of the Republic' and the words 'in subsection 30 (2²)' are replaced with the words 'and subsection 33 (4) of the Classified Information of the Foreign States Act.'

7) Subsection (7) with the following wording shall be added to § 54¹ of the Act:

'(7) A candidate for the position of the Chief Justice of a Supreme Court may be appointed for office, supported by data collected as the result of security vetting, within nine months as of the communication of information collected as the result of security vetting to a competent authority or constitutional institution by an agency performing security vetting. A candidate for the position of the Chief Justice of a Supreme Court may be appointed to the office after the expiry of this term only after passing another security vetting.

§ 75. Amendment of Code of Criminal Procedure

The Code of Criminal Procedure (RT I 2003, 27, 166; 2006, 48, 360) shall be amended as follows:

- a. the words 'or classified information of a foreign state' are added after the words 'business secret' in clause 12 (1) 1);
- b. the words 'and classified information of foreign states' shall be added to the title of § 73 after the words 'state secret';
- c. the words 'and classified information of foreign states act' are inserted in subsection 73 (1) after the words 'Act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387; 2003, 13, 67)';
- d. the words 'or classified information of a foreign state' are added after the words 'state secret' in subsections 73 (2) and (3);

e. the words ‘state secrets’ are replaced with the words ‘classified information of a foreign state’ in clause 121 (2) 3);

f. Section 224 (7) shall be amended and worded as follows:

‘(7) Upon the counsel’s request, the court will be supplied with a media containing state secrets or classified information of a foreign state, not added to a criminal file, that is used as an evidence for the purposes of criminal proceedings, to be reviewed as provided by the State Secrets and Classified Information of Foreign States Act. A record concerning the introduction of a medium containing state secret or classified information of a foreign state is made to the criminal file.’.

§ 76. Amendment of Taxation Act

The words ‘state secret’ are replaced with the words ‘obligation to safeguard a state secret or classified information of a foreign state’ in clause 64 (1) 7) of the Taxation Act (RT I 2002, 26, 150; 2006, 43, 3259).

§ 77. Amendment of Peace-Time National Defence Act

The Peace-Time National Defence Act (RT I 2002, 57, 354; 2006, 50, 374) shall be amended as follows:

a. clause 14) with the following wording shall be added to subsection 10 (2):

‘14) shall organise and check the protection of classified information of foreign states as provided by the State Secrets and Classified Information of Foreign States Act.’;

b. Subsection (3) and (4) with the following wording are added to § 10 of the Act:

‘(3) The officials of the Ministry of Defence, organising and checking the protection of classified information of foreign states, are entitled to carry a service weapon and use it as provided by the State Secrets and Classified Information of Foreign States Act.

(4) The types of service weapons to be used for the purposes of organisation and checking of classified information of foreign states and the procedure for their handling shall be established with the regulation of a Minister of Defence.'

§ 78. Amendment of State Budget Act

The words 'state secret' in subsection 4 (6) of the State Budget Act (RT I 1999, 55, 584; 2004, 22, 148) shall be replaced with the words 'state secret or classified information of foreign states'.

§ 79. Amendment of Public Procurement Act

The words 'and classified information of foreign states act' are added in subsection 4 (1) after the words 'Act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387; 2003, 13, 67; 23, 147)' and the words 'or classified information of a foreign state' are added after the words 'state secret'.

§ 79. Amendment of National Defence Duties Act

The words 'and classified information of a foreign state' are added after the words 'business secret' in § 5 of the National Defence Duties Act (RT I 1995, 25, 352; 2005, 39, 308).

§ 80. Amendment of Riigikogu Rules of Procedure Act

The words 'or classified information of a foreign state' are added after the words 'state secret' in subsection 146 (9) of the Riigikogu Rules of Procedure Act (RT I 2003, 24, 148; 2006, 12, 80).

§ 81. Amendment of Riigikogu Internal Rules Act

§ 14¹ of the Riigikogu Internal Rules Act (RT 1992, 46, 582; I 2003, 4, 22) shall be amended and worded as follows:

‘§ 14¹. Members of the Riigikogu have the right for access to state secrets in order to perform their duties.

If so provided in a justified decision of the Prime Minister or relevant minister, members of the Riigikogu may be refused the access for specified classified information of a foreign state or state secret, if:

- a. the state secret concerns a source of security related information;
- b. the state secret concerns a method of action, adopted by a security authority and is still being used;
- c. the state secret concerns the method for collection of information, adopted by a security authority as provided by § 25 or 26 of the Security Authorities Act and is still in process; or
- d. if disclosure of a state secret may endanger the performance of obligations, specified in clauses 8 (1) 2), 3) and 4) of the Surveillance Act.

§ 82. Amendment of State Audit Office Act

The State Audit Office Act (RT I 2002, 21, 117; 2006, 48, 357) shall be amended as follows:

- 1) Subsection 18 (1) shall be amended and worded as follows:

‘(1) Candidates for the position of State Auditor must pass security vetting before being appointed as a State Auditor, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.’;

- 2) the words ‘in the Surveillance Act (RT I 1994, 16, 290; 1995, 15, 173; 1996, 49, 955; 1997, 81, 1361; 93, 1557; 1998, 47, 698; 50, 753; 51, 756; 61, 981; 98/99, 1575; 101, 1663; 1999, 16, 271; 31, 425; 95, 845; 2000, 35, 222; 40, 251; 102, 671; 2001, 3, 9; 7, 17)’ in subsection 18 (3) shall be replaced with the words ‘in the Security Authorities Act’;

- 3) the words “‘top secret’ level’ in subsection 18 (4) shall be replaced with the words ‘at ‘top secret’ level’;

4) the words ‘committee for protection of state secrets’ in subsection 18 (6) shall be replaced with the words ‘Security Committee of the Government of the Republic’ and the words ‘in subsection 30 (2²)’ are replaced with the words ‘and subsection 33 (4) of the Classified Information of the Foreign States Act’;

5) Subsection (7) with the following wording shall be added to § 18:

‘(7) A candidate for the position of the State Auditor may be appointed for office, supported by data collected as the result of security vetting, within nine months as of the communication of information collected as the result of security vetting to a competent authority or constitutional institution by an agency performing security vetting. A candidate for the position of the State Auditor may be appointed to the office after the expiry of this term only after passing another security vetting.’;

6) Section 25¹ with the following wording shall be added to the Act:

‘§ 25¹. Access of a State Auditor to State Secrets and Classified Information of a Foreign State

(1) A State Auditor shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging their functions.

(2) If, under an international agreement, the performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to a State Auditor.

(3) For passing security vetting, a State Auditor is required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the security authorities surveillance committee of the Riigikogu.

- (4) The security authorities surveillance committee of the Riigikogu shall appoint an authority performing security vetting that shall be communicated the documents, specified in subsection (3) of this section.
- (5) The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to a State Auditor three months as of the receipt of documents, specified in subsection (3) of this section to the security authorities' surveillance committee of the Riigikogu for deciding whether a State Auditor has passed security vetting. A Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under the procedure specified in the State Secrets and Classified Information of Foreign States Act.;
- 7) The words 'information deemed as classified under the State Secrets Act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643) or other Acts' are replaced with the words 'information classified as restricted.';
- 8) Subsection 43 (7) shall be amended and worded as follows:

'(7) The right to examine media containing state secrets or classified information of foreign states is granted to the officials of the State Audit Office, holding the right for access to the respective level of state secrets and classified information of foreign states, as provided by the State Secrets and Classified Information of Foreign States Act.';
- 9) the words 'classified information of foreign states' are added after the words 'banking secret' in subsection 47 (2);
- 10) the words 'classified information of foreign states' are added after the words 'banking secret' in subsection 51 (1);
- 11) the words 'or classified information of foreign states' are added after the words 'state secret' in subsection 52 (4).

§ 83. Repealing of State Secrets Act

The State Secrets Act (RT I 1999, 16, 271; 2005, 64, 482) is repealed.

§ 84. Amendment of State Assets Act

The words ‘or classified information of foreign states’ are added after the words ‘state secret’ in subsection 3 (1¹) of the State Assets Act (RT I 1995, 22, 327; 2005, 39, 308).

§ 85. Amendment of the Strategic Goods Act

The Strategic Goods Act (RT I 2004, 2, 7; 2006, 50, 376) shall be amended as follows:

- 1) The words ‘and classified information of foreign states act’ are added in subsection 9 (2) after the words ‘Act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387; 2003, 13, 67; 23, 147; 2004, 2, 7; 43, 300)’.
- 2) The words ‘and classified information of foreign states’ are added after the words ‘state secret’ in subsection 10 (2).

§ 86. Amendment of the War-Time National Defence Act

Subsection 12 (1¹) of the War-Time National Defence Act (RT I 1994, 69, 1194; 2003, 13, 69) is repealed.

§ 87. Amendment of the Customs Act

The words ‘act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387; 2003, 13, 67; 23, 147; 2004, 2, 7) are replaced with the words ‘and classified information of foreign states act’ in subsection 58 (2) of the Customs Act (RT I 2004, 28, 188).

§ 88 Amendment of Civil Code of Procedure

The Civil Code of Procedure (RT I 2005, 26, 197; 2006, 48, 360) shall be amended as follows:

- 1) the words ‘act (RT I 1999, 16, 271; 82, 752; 2001, 7, 17; 93, 565; 100, 643; 2002, 53, 336; 57, 354; 63, 387; 2003, 13, 67; 23, 147; 2004, 2, 7; 43, 300; 46, 329; 54, 387) are replaced with the words ‘and classified information of foreign states act’ in subsection 38 (1);

- 2) the words 'or classified information of foreign states' in required case are added after the words 'state secret' throughout subsection 259 (4);
- 3) the words 'or classified information of a foreign state' are added after the words 'business secret' in subsection 275 (1).

§ 89. Amendment of Witness Protection Act

Clause 4), worded as follows, shall be added to subsection 12 (3) of the Witness Protection Act (RT I 2005, 39, 307; 2006, 31, 233):

'4) if this is not accompanied by a considerable threat for the protection of state secrets and classified information of foreign states.'

§ 90. Amendment of the Government of the Republic Act

§ 3¹ of the Government of the Republic Act (RT I 1995, 94, 1628; 2006, 14, 111) shall be amended and worded as follows:

§ 3¹. Access of a Members of the Government of the Republic to State Secrets and Classified Information of a Foreign State

- (1) Members of the Government of the Republic shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging their functions.
- (2) If, under an international agreement, the performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to a member of the Government of the Republic.
- (3) For passing security vetting, members of the Government of the Republic are required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain

information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the security authorities' surveillance committee of the Riigikogu.

- (4) The security authorities' surveillance committee of the Riigikogu shall appoint an authority performing security vetting with respect to a member of the Government of the Republic that shall be communicated the documents, specified in subsection (3) of this section. An agency within the governing area of a ministry, chaired by a minister to be checked, must not be appointed to perform security vetting on a minister.
- (5) The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to a member of the Government of the Republic within three months as of the receipt of documents, specified in subsection (3) of this section to the security authorities' surveillance committee of the Riigikogu for deciding whether a judge has passed security vetting. A Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under the procedure specified in the State Secrets and Classified Information of Foreign States Act.

§ 91. Amendment of Foreign Service Act

Section 58 of the Foreign Services Act (RT I 2006, 26, 193; 2006, 49, 370) shall be repealed.

§ 92

§ 93. Amendment of Chancellor of Justice Act

The Chancellor of Justice Act (RT I 1999, 29, 406; 2006, 48, 357) shall be amended as follows:

- a. Subsection 6¹ (1) of the Act shall be amended and worded as follows:

‘(1) Candidates for the position of Chancellor of Justice must pass security vetting before being appointed, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.’;

b. the words ‘in the Surveillance Act (RT I 1994, 16, 290; 1995, 15, 173; 1996, 49, 955; 1997, 81, 1361; 93, 1557; 1998, 47, 698; 50, 753; 51, 756; 61, 981; 98/99, 1575; 101, 1663; 1999, 16, 271; 31, 425; 95, 845; 2000, 35, 222; 40, 251; 102, 671; 2001, 3, 9; 7, 17)’ in subsection 6¹ (3) shall be replaced with the words ‘in the Security Authorities Act’;

c. the words ‘‘top secret’ level’ in subsection 6¹ (4) shall be replaced with the words ‘at ‘top secret’ level’;

d. the words ‘committee for protection of state secrets’ in subsection 6¹ (6) shall be replaced with the words ‘Security Committee of the Government of the Republic’ and the words ‘in subsection 30 (2²)’ are replaced with the words ‘and subsection 33 (4) of the Classified Information of the Foreign States Act’;

e. Subsection (7) with the following wording shall be added to § 6¹:

‘(7) A candidate for the position of Chancellor of Justice may be appointed for office, supported by data collected as the result of security vetting, within nine months as of the communication of information collected as the result of security vetting to the President of the Republic by an agency performing security vetting. A candidate for the position of Chancellor of Justice may be appointed to the office after the expiry of this term only after passing another security vetting.’

f. Section 11¹ with the following wording shall be added to the Act:

‘§ 11¹. Access of a Chancellor of Justice to State Secrets and Classified Information of a Foreign State

- (1) A Chancellor of Justice shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging his/her functions.
 - (2) If, under an international agreement, the performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to a Chancellor of Justice.
 - (3) For passing security vetting, a Chancellor of Justice is required to complete the application form for a Security Personnel Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the security authorities' surveillance committee of the Riigikogu.
 - (4) The security authorities' surveillance committee of the Riigikogu shall appoint an authority performing security vetting with respect to the Chancellor of Justice that shall be communicated the documents, specified in subsection (3) of this section.
 - (5) The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to a Chancellor of Justice within three months as of the receipt of documents, specified in subsection (3) of this section to the security authorities' surveillance committee of the Riigikogu whether a Chancellor of Justice has passed security vetting. A Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under the procedure specified in the State Secrets and Classified Information of Foreign States Act.;
- g. the words 'classified information of foreign states' shall be added after the words 'state secrets' in § 13;

h. §§ 37¹ and 37², worded as follows, shall be added to the Act:

‘§ 37¹. Security Vetting with Respect to Deputy Chancellor of Justice-Adviser

- (1) Candidates for the position of Deputy Chancellor of Justice-Adviser must pass security vetting before being appointed, except when holding a valid Personnel Security Clearance classified as ‘top secret’ or if holding an office, when becoming a candidate, granting access to all the classification levels of state secrets by virtue of office.
- (2) The status of a candidate for the position of Deputy Chancellor of Justice-Adviser is acquired by a person who was asked to run for the office by the Chancellor of Justice and who has been granted written consent for running for the office.
- (3) Security vetting with respect to a Deputy Chancellor of Justice-Adviser shall be performed by the Security Police Board, as provided by the Security Authorities Act.
- (4) For passing security vetting, a Deputy Chancellor of Justice-Adviser is required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the Security Police Board through the Office of the Chancellor of Justice.
- (5) The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to a judge within three months as of the receipt of documents, specified in subsection (3) of this section, to the Office of the Chancellor of Justice, adding its opinion regarding the compliance of the candidate for the position of Deputy Chancellor of Justice-Adviser with the requirements established for the issue of a Personnel Security Clearance. A candidate for the position of Deputy Chancellor of Justice-Adviser may be appointed for office, supported by data collected as the result of security

vetting, within nine months as of the communication of information collected as the result of security vetting to a competent authority or constitutional institution by an agency performing security vetting. A candidate for the position of Deputy Chancellor of Justice-Adviser may be appointed to the office after the expiry of this term only after passing another security vetting.

§ 37². Access of Deputy Chancellor of Justice-Adviser to State Secrets and Classified Information of a Foreign State

- a. A Deputy Chancellor of Justice-Adviser shall be granted right for access to state secrets and classified information of foreign states by virtue of office and under the Constitution and law of the Republic of Estonia and legislation issued on the basis thereof for discharging their functions.
- b. If, under an international agreement, the performance of security vetting is a mandatory prerequisite for granting right for access to classified information of a foreign state, security vetting shall be performed with respect to a Deputy Chancellor of Justice-Adviser.
- c. For passing security vetting, a Deputy Chancellor of Justice-Adviser is required to complete the application form for a Personnel Security Clearance and sign a consent that shall entitle an agency competent to conduct security verification to obtain information concerning the person from natural and legal persons and from institutions and bodies of local government, submitting the documents to the security authorities' surveillance committee of the Riigikogu through the Office of the Chancellor of Justice.
- d. Security authorities' surveillance committee of the Riigikogu shall appoint an authority performing security vetting that shall be communicated the documents, specified in subsection (3) of this section.
- e. The agency performing security vetting shall communicate the documents, collected when performing security vetting with respect to a Deputy Chancellor of Justice-Adviser within three months as of the receipt of documents, specified in subsection (3) of this section to the

security authorities' surveillance committee of the Riigikogu for deciding whether a judge has passed security vetting. A Personnel Security Clearance Certificate for Access to Foreign Classified Information is issued under the procedure specified in the State Secrets and Classified Information of Foreign States Act.;

§ 94. Entry into Force

This Act shall enter into force on 1st January 2008.

President of the Riigikogu

Toomas Varek

Tallinn, '...' 2006

Initiated by the Government of the Republic

On 4th December 2006, No. 1-6/146