Issuer:	Riigikogu
Type:	act
In force from:	01.01.2025
In force until:	In force
Translation published:	06.01.2025

State Secrets and Classified Information of Foreign States Act

Passed 25.01.2007
RT I 2007, 16, 77
Entry into force 01.01.2008

Amended by the following acts

Passed	Published	Entry into force
14.06.2007	RT I 2007, 44, 316	14.07.2007
04.12.2007	RT I 2007, 68, 420	29.12.2007
19.06.2008	RT I 2008, 35, 213	01.01.2009
17.12.2008	RT I 2009, 4, 24	01.03.2009
17.12.2008	RT I 2009, 5, 35	01.07.2009
15.06.2009	RT I 2009, 39, 262	24.07.2009
26.11.2009	RT I 2009, 62, 405	01.01.2010
22.04.2010	RT I 2010, 22, 108	01.01.2011 entry into force on the date determined in the Decision of the Council of the European Union regarding the abrogation of the derogation established in respect of the Republic of Estonia on the basis provided for in Article 140 (2) of the Treaty on the Functioning of the European Union, Council Decision 2010/416/EU of 13 July 2010 (OJ L 196, 28.07.2010, p. 24 – 26).
21.10.2010	RT I, 08.11.2010, 3	18.11.2010
27.01.2011	RT I, 17.02.2011, 2	01.01.2012
15.06.2011	RT I, 08.07.2011, 8	22.07.2011
07.12.2011	RT I, 22.12.2011, 2	01.01.2012
29.01.2014	RT I, 18.02.2014, 1	01.08.2014, The words 'defence forces' have been replaced by the words 'Defence Forces' in the corresponding case throughout the Act
19.02.2014	RT I, 13.03.2014, 4	01.07.2014
12.06.2014	RT I, 21.06.2014, 11	01.07.2014
19.06.2014	RT I, 29.06.2014, 109	01.07.2014, the official titles of the ministers have been replaced on the basis of subsection 4 of § 107³ of the Government of the Republic Act.
18.02.2015	RT I, 06.03.2015, 9	16.03.2015, the words “the Headquarters of the Defence Forces’ have been replaced by the words ‘a structural unit designated in the statutes of the Defence Forces’ in the corresponding case
11.02.2015	RT I, 12.03.2015, 1	01.01.2016
19.10.2016	RT I, 04.11.2016, 1	01.01.2017
20.04.2017	RT I, 05.05.2017, 1	01.07.2017

13.06.2018	RT I, 29.06.2018, 3	01.07.2018
20.02.2019	RT I, 13.03.2019, 2	15.03.2019
20.04.2020	RT I, 06.05.2020, 1	07.05.2020, applied in part retroactively from 01 March 2020
11.01.2023	RT I, 27.01.2023, 1	01.04.2023
15.02.2023	RT I, 07.03.2023, 7	01.04.2023, in part 01.01.2024
13.02.2023	RT I, 07.03.2023, 2	01.05.2023; in the text the words „possessor of information“ have been replaced by part of the text ”agency, constitutional institution or legal person“, and the part of the text ”agency, constitutional institution and legal person“ with the words „processing unit“
20.11.2024	RT I, 12.12.2024, 1	01.01.2025

Chapter 1
GENERAL PROVISIONS

§ 1. Purpose of Act

The purpose of this act is to ensure the security and foreign relations of the Republic of Estonia, protecting state secrets and classified information of foreign states from disclosure and becoming 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 state secrets and classified information of foreign states, and the bases for classification and the changing of related terms; the grounds for the protection of state secrets, classified information of foreign states and classified media and liability incurring from the violation of this Act.

(2) Provisions of the Administrative Procedure Act apply to the administrative procedures 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 or foreign relations of the Republic of Estonia 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 an organisation or institution established under an international agreement (hereinafter collectively referred to as ‘originator of classified information of a foreign state’) which is released 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) [Repealed – RT I, 07.03.2023, 2 – entry into force 01.05.2023]
5) “need for access” means the need to process a state secret or classified foreign information if such 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 of access” means a natural person’s right to process state secrets or classified information of foreign states by virtue of office or based on a decision of the head of the institution, a Personnel Security Clearance or a Personnel Clearance Certificate, applicable witness protection measures or an order of an investigative body, the Prosecutor’s Office or a court, or a decision of an agency which performs security vetting;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
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 therefor;
9) “processing system” means an electronic communications network or information system which is used for electronic processing of information;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

10) “INFOSEC” means the ensuring of the availability, confidentiality and integrity of 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 has not been appointed, elected or employed under the employment contract to a post or employment at a government authority or a state authority governed by a government authority, Eesti Pank or the Estonian Defence League;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
13) “National Security Authority” means a structural unit of a governmental authority designated by the Government of the Republic, which is assigned to organise and supervise the protection of classified information of foreign states;
[RT I, 04.11.2016, 1 – entry into force 01.01.2017]
14) “security area” means an area where state secrets classified as ‘confidential’, ‘secret’ or ‘top secret’ or classified information of foreign states and medium containing such information is processed.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]
15) „processing unit“ – an agency, constitutional institution or legal person or a natural person processing classified information based on a facility security clearance.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

§ 4. Authorisation of secretary general

A minister may authorise the secretary general 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 3 of subsection 3 of § 13 and subsection 5 of § 27 of this Act.

Chapter 2
STATE SECRET

Subchapter 1
State secret levels and types

§ 5. Classification of state secrets

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 collected and prepared by the Strategic Goods Commission operating at the Ministry of Foreign Affairs, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information is classified at the ‘secret’ or lower level for a maximum period of fifty years;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
3) items of information created by a foreign relations institution which, once communicated, would considerably damage foreign relations of the Republic of Estonia, except for information specified in clause 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;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

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 the stockpile necessary for organisation of mobilisation, except information the disclosure of which would not damage the security of the Republic of Estonia, or which is subject to disclosure under a treaty. Such information is classified at the ‘secret’ or lower level for a maximum period of thirty years;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
4) items of information concerning military weapons, ammunition and munitions of the Estonian Defence Forces (hereinafter the Defence Forces) and the Estonian Defence League (hereinafter 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 a treaty. Such information is classified at the ‘secret’ or lower level for a maximum period of thirty years;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
5) [Repealed – RT I 2008, 35, 213 – entry into force 01.01.2009]
5^1) information collected from the radar information and surveillance systems of the Defence Forces, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information is classified at the ‘secret’ or lower level for a maximum period of thirty years;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
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 thirty years;
[RT I 2009, 4, 24 – entry into force 01.03.2009]
6^1) information regarding the characteristics, design, manufacture and adaptation of an item for military purpose, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information is classified at the ‘secret’ or lower level for up to 30 years;
[RT I, 12.12.2024, 1 - entry into force 01.01.2025]
7) items of information collected and synthesised by a structural unit of the Defence Forces which deals with intelligence and counterintelligence, 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.
[RT I 2008, 35, 213 – entry into force 01.01.2009]
8) items of information concerning the composition, functions and distribution of the budget of a structural unit of the Defence Forces exercising the authority specified in clauses 1, 2 and 5 of subsection 1 and subsection 2 of § 37 of the Estonian Defence Forces Organisation Act, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information is classified at the ‘secret’ or lower level for a maximum period of fifty years;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
9) [Repealed – RT I 2008, 35, 213 – entry into force 01.01.2009]
10) items of information concerning the collection of covert information by a structural unit of the Defence Forces, specified in clauses 1 and 2 of subsection 1 and subsection 2 of § 37 of the Estonian Defence Forces Organisation Act, which deals with intelligence and counter-intelligence, including the information concerning the methods 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;
[RT I 2008, 35, 213 – entry into force 01.01.2009]
11) items of information concerning international co-operation concerning intelligence and counterintelligence, 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;
[RT I 2008, 35, 213 – entry into force 01.01.2009]
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 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 a person specified in this clause but not earlier than fifty years since 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 classification of the information;
4) items of information concerning the structure, composition and functions of the witness protection sub-unit of the Police and Border Guard Board, 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;
[RT I 2009, 62, 405 – entry into force 01.01.2010]
5) items of information concerning the assets and distribution of the budget of the witness protection sub-unit of the Police and Border Guard Board, 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;
[RT I 2009, 62, 405 – entry into force 01.01.2010]
6) items of information concerning the methods and tactics of the application of witness protection measures, 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 measures, 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 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 the public use of such information in an emergency situation or a state of war;
9) [Repealed – RT I, 12.03.2015, 1 – entry into force 01.01.2016]
10) [Repealed – RT I 2009, 39, 405 – entry into force 24.07.2009]
11) Information regarding the conduct of defence operations of the personal protection unit of the Police and Border Guard Board, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information is classified at the 'restricted' level for a maximum period of twenty-five years or until the need to provide personal protection or the provision of personal protection ceases;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
12) Information regarding the weapons, ammunition, special equipment, and supply of the special tactical unit of the Police and Border Guard Board, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information is classified at the 'restricted' level for a maximum period of twenty-five years.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

§ 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 the 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 the security authorities and distribution of the 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 'top secret' or lower level for a maximum period of twenty years. Classification shall expire upon the 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 clause 1 of § 8 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 collected 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 composition, functions and distribution of the budget of structural units of a security authority, 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 a person recruited for secret co-operation by the security authority and an undercover staff official or employee of the security authority, except the information specified in clause 2 of § 8 of this Act. Such information shall be classified as top secret for a maximum period of seventy-five years. Classification shall expire if twenty years have passed since the death of a person but not earlier than fifty years since classification of the information;
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]
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 Estonian Internal Security Service (hereinafter Internal Security Service) pursuant to the procedure provided for in clause 1 of subsection 2 of § 5 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 that pursuant to the currently valid law of the Republic of Estonia is punishable as a criminal offence 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 Riigikogu 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;
11) information available from document registers of security authorities. Such information shall be classified at the 'secret' level for a maximum period of twenty-five years or at a higher level and for a longer term if the register concerned contains information with the appropriate classification level and term.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

§ 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, Eesti Pank, the Defence League, the government authorities assigned by a regulation of the Government of the Republic Government of the Republic Under the Procedure for Protection of State Secrets and Classified Information of Foreign States and the authorities governed by such government authorities, 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 is classified at the 'confidential' or lower level for a maximum period of thirty years.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
1^1) items of information concerning the security and alarm systems and protective measures of national defence objects for the purposes of the National Defence Act, except objects specified in clause 1 of this section and national defence objects essential for ensuring public order, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'restricted' level for a maximum period of twenty years;
[RT I, 12.03.2015, 1 – entry into force 01.01.2016]
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 exercising the authority specified in clauses 1, 2 and 5 of subsection 1 of § 37 of the Estonian Defence Forces Organisation 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 until the expiry of the possession of a building or premises;
[RT I, 18.02.2014, 1 – entry into force 01.08.2014]
4) items of information concerning weapons and munitions 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 weapons or munitions warehouse;
5) items of information concerning evacuation of the classified media of a possessor of a 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 within a secure area of a possessor of the 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;

7) information concerning the carriage of cash by Eesti Pank, except for 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 ten years;
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]
8) information concerning organisation of and the requirements for uninterrupted communication, except information the disclosure of which would not damage the security of the Republic of Estonia. Such information shall be classified at the 'restricted' level for a maximum period of twenty-five years.
[RT I, 17.02.2011, 2 – entry into force 01.01.2012]
9) [Repealed – RT I, 07.03.2023, 2 – entry into force 01.05.2023]

§ 11. Sub-classes of information regarded as state secrets and establishment of terms and levels of classification thereof

(1) Sub-classes of information specified as state secret in § 6, clauses 1–8 and 10–12 of §7, clauses 1, 2 and 4–12 of §8, clauses 1–6 and 9–10 of § 9 and § 10 of this Act and the terms and level of classification of such information are established by a regulation of the Government of the Republic. The term of classification of the sub-classes of classified information may be linked to the occurrence of a particular event, taking into consideration the maximum term of classification specified in this Act.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(2) The level and term of classification of information, specified in clause 6 of § 7 of this Act, shall be established separately for each invention and study by the minister in charge of the policy sector. The Ministry of Defence shall communicate to the Patent Office information on the topics of the technical field that may be important for national defence purposes and therefore be subject to classification. Such information shall be classified at the 'restricted' level, as appropriate, or as information intended for internal use only.
[RT I 2009, 4, 24 – entry into force 01.03.2009]

(3) Information specified in § 6, clauses 1–4, 6, 7 and 10–12 of §7, clauses 1 and 4–12 of §8, clauses 1–6 and 9 and 10 of § 9 and § 10 of this Act, the disclosure of which would not damage the security of the Republic of Estonia, is treated as information intended for internal use in case restriction of access to such information is required under an agreement with a private person, foreign state or international organization, or in case the disclosure of such information would damage the foreign relations of the state or discharge of the functions of the processing unit arising from law.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

Subchapter 2
Expiry of classification of state secrets, modification of classification bases and term

§ 12. Expiry of classification of state secret

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

§ 13. Premature declassification of information classified as 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, classified as state secret, specified in clauses 2, 3 and 7 of §8 and clauses 7 and 8 of § 9of this Act, is only permitted during the lifetime of the person concerned upon the written consent of the concerned person to the extent specified by him or her, except in case the person has been convicted of intentionally committed criminal offence against the state or a crime against humanity.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(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 or the head of an authority with the authorisation of the minister – in the case of a state secret created within the area of government of the ministry, or in case of the authorisation by the respective authority, except a state secret entered in a medium submitted to the Government of the Republic or government committee or in case of authorisation to the minister for adopting a decision;

[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
4) the Chief Justice of the Supreme Court – in the case of a state secret created by courts;
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 and its subsidiaries;
8) the State Secretary – in the case of a state secret created by the Government Office, except a state secret entered in a medium submitted to the Government of the Republic or government committee for adopting a decision;
9) the head of a security authority – in the case of a state secret created by a security authority, except a state secret entered in a medium submitted to the Government of the Republic or a respective minister for adopting a decision. Declassification of a state secret takes place before the intended term of expiry in case this is necessary for discharging a function of a security authority and only to the extent that does not endanger the security of individuals who are specified in that information or who participated or are participating in the collection of the information;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
10) the head of a surveillance authority – in the case of a state secret created by a surveillance authority specified in clause 1 of §8 of this Act, except a state secret entered in a medium submitted to the Government of the Republic or a respective minister for adopting a decision. Declassification of a state secret takes place before the intended term of expiry in case this is necessary for discharging a function of a surveillance authority and only to the extent that does not endanger the security of individuals who are specified in that information or who participated or are participating in the collection of the information;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
11) the Commander of the Defence Forces or a commander authorised by the Commander of the Defence Forces – in the case of a state secret specified in clauses 7, 10 and 11 of § 7of this Act, except a state secret entered in a medium submitted to the Government of the Republic, a government committee, or a respective minister for adopting a decision. Declassification of a state secret takes place before the intended term of expiry in case this is necessary for discharging a function of intelligence and counterintelligence and only to the extent that does not endanger the security of individuals who are specified in that information or who participated or are participating in the collection of the information.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(4) The Government of the Republic shall decide on the premature declassification of information that 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 media shall be established by a regulation of the Government of the Republic in the Procedure for Protection of State Secrets and Classified Information of Foreign States.

§ 14. Procedure for extension of term for classification of information classified as 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 established by this Act and legislation issued on the basis thereof, the term for the classification of information may be extended for five-year periods, but not for more than seventy-five years in all. The term for the classification of the information specified in clause 8 of § 9 of this Act may not be extended.

(2) The decision to extend a term for the 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 courts;
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 the Bank of Estonia – in the case of a state secret created by Eesti Pank and its subsidiaries.
7) the minister – in the case of a state secret created in the area of government of the ministry, except a state secret entered in a medium submitted to the Government of the Republic or a government committee for adopting a decision;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
8) the State Secretary – in the case of a state secret created by the Government Office, except a state secret entered in a medium submitted to the Government of the Republic or government committee for adopting a decision;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
9) the head of a security authority – in the case of a state secret created by a security authority specified in §§ 6, 7, 9 and 10 of this Act, except a state secret entered in a medium submitted to the Government of the Republic, government committee or a respective minister for adopting a decision.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(3) The Government of the Republic shall decide on the extension of the term for the classification of information, which is classified as a state secret, not specified in subsection 2 of this section.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(4) The procedure for filing a request for the extension of the term for the classification of information which is classified as a state secret, notification of the intention of extension of the term for classification, contesting extension of the term for classification, notification of extension of the term for classification and marking the appropriate media shall be established by a regulation of the Government of the Republic in the Procedure for Protection of State Secrets and Classified Information of Foreign States.

§ 15. Declassification of information processed as state secret with no legal grounds and changing level of classification of information classified as state secret, basis and term of classification

(1) The Government of the Republic shall declassify the classification of 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 included in a medium to be submitted to the Government of the Republic or a government committee for the adoption of a decision.

(2) A natural person outside the service or institution serving as the originator of the information or an individual or his or her deputy assigned by an agency, constitutional institution or legal person that are originators of information assigned under the procedure provided in subsection 2 of § 20 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 or the originator of the information is no longer entitled to process a state secret, the minister in charge of the policy sector 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.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(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, legal 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 the declassification of the information or changing the level of classification, notification of declassification or changing the level of classification and marking of the respective media shall be established by a regulation of the Government of the Republic in the Procedure for Protection of State Secrets 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 the incorrect level, on wrong legal grounds or for a wrong term has been proven by a court ruling or a ruling on misdemeanour, the possessors of media bearing such information shall immediately mark such media pursuant to subsection 4 of this section under the procedure established by a regulation of the Government of the Republic.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

Subchapter 3
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 the INFOSEC procedure;
3) protection of state secrets against unlawful disclosure;
4) periodic inspection of the existence and integrity of media;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
5) imposition of disciplinary, misdemeanour or criminal liability for violation 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) The 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 term of classification of a state secret stored on the medium. If state secrets of different types and with different terms of classification 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 with no right of access to state secrets

(1) A person with no right of 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 Estonian Internal Security Service (hereinafter Internal Security Service) once realising he or she is in possession of a state secret or classified medium. The person is required to give the classified medium promptly to the Internal Security Service.

(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 person is required to maintain the confidentiality thereof and promptly notify the Internal Security Service after he or she realised or should have realised that 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 2 of § 20 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 or her disposal, required to protect the classified medium from disclosure and from access by persons with no right of access and need to know, until the classified medium can be handed over.

§ 19. Duties of persons with right of access to state secrets and facility security clearance

(1) A person with the right of access to state secrets or a Facility Security Clearance is required to:
1) maintain the confidentiality of state secrets which become known to him or her;
2) protect classified media in his or her possession from disclosure and access by unauthorised persons with no right of access or need to know;
3) notify immediately an agency, a constitutional institution or legal person in whose service the person obtained the right of access or a Facility Security Clearance due to a service or some other contractual relationship, and the Internal Security Service of any person who attempted or is attempting in any way to obtain unlawful access to state secrets;
4) notify the authority organizing the protection of state secrets of the institution at the place of performance of work or service tasks and the authority that supervises compliance with the requirements of this Act and legislation issued on the basis thereof, the person organizing the protection of state secrets of the institution at the place of performance of work or service tasks, and the Internal Security Service immediately of any violation of the requirements of this Act or legislation issued on the basis thereof that has become known to them;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
5) take measures upon illegal disclosure of a state secret or becoming known thereof to an unauthorised person with no right of access to state secrets to avoid the damages potentially resulting from such disclosure or communication;
6) notify immediately the corresponding agency which is competent to perform a security vetting of the address of his or her place of stay and other contact information when staying in a foreign state for a period longer than three months;
7) [Repealed – RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(2) A natural person with the right of access is required to notify an agency, a constitutional institution or legal person, in whose service the person obtained the right of access, of the stay in a foreign state outside employment or service duties, which is subject to notification requirement. The provisions of this subsection shall not be applied to the persons specified in subsection 1 of § 27 of this Act.
[RT I, 06.03.2015, 9 – entry into force 16.03.2015]

(3) The minister in charge of the policy sector of government of the Ministry of the Interior shall establish, for the prevention of unlawful attempts of access to state secrets, a list of foreign states which are subject to the notification requirement specified in subsection 2 of this section. A member state of the European Union, Schengen Agreement or NATO is not subject to the notification requirement.
[RT I, 06.03.2015, 9 – entry into force 16.03.2015]

(4) A natural person with the right of access notifies, in a form reproducible in writing, the person organising the protection of state secrets of the processing unit, in whose service the person obtained the right of access based on service or other contractual relationship, at the latest five working days before the beginning of the intended travel. A natural person with the right of access, who is in the employment or service relationship with the processing unit that does not have a person organizing the protection of state secrets or with the originator of classified information, notifies the Internal Security Service.The unexpected stay in a foreign state must be notified of without delay. The notice specifies the name of the person, communication means, foreign state and the period and reason for staying there.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(5) A person organising the protection of state secrets of an agency, a constitutional institution or legal person, in whose service the person obtained the right of access, or an official of a security authority shall explain without undue delay to the person with the right of access the risks to his or her security or the security of the state related to the travel to a foreign state and shall give recommendations related to travelling to a foreign state.
[RT I, 06.03.2015, 9 – entry into force 16.03.2015]

(6) An agency, a constitutional institution or legal person, in whose service the person obtained the right of access shall keep notices submitted based on subsection 2 of this section up to the end of the calendar year following the expiry of validity of the right of access of the person. A security authority may use the data collected based on subsection 2 of this section to check the facts specified in subsections 1 and 2 of § 32 of this Act.
[RT I, 06.03.2015, 9 – entry into force 16.03.2015]

(7) The obligations provided in clause 6 of subsection 1 and subsections 2 and 4 of this section do not apply to the person who has obtained the right of access on the basis provided in § $30^1$of this Act.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

§ 20. Duties of person in possession of classified information

(1) A person in possession of classified information is required to adopt suitable organisational, physical and INFOSEC security measures for the protection of state secrets.

(1^1) A possessor of classified information shall have the right to apply special measures of state supervision provided for in §§ 47 and 52 of the Law Enforcement Act for entering into the security area of classified information on the basis of and in the procedure provided for in the Law Enforcement Act. Application of measures specified in §§ 47 and 52 of the Law Enforcement Act shall not be recorded.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

(1^2) During the stay in the security area of classified information the possessor of classified information shall have the right to apply special measures of state supervision provided for in §§ 48, 49 and 52 of the Law Enforcement Act on the basis of and in the procedure provided for in the Law Enforcement Act.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

(1^3) During the stay in the security area of classified information the possessor of classified information shall have the right to use physical force upon application of special measures of state supervision provided for in §§ 48, 49 and 52 of the Law Enforcement Act on the basis of and in the procedure provided for in the Law Enforcement Act.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

(2) The head or a directing body of an agency, institution, or a legal person in possession of state secrets 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 a structural unit specified in subsection 2 of this section shall be directly subordinate to the head or directing body of an agency, constitutional institution, or legal person and to the Secretary General in ministries, in issues concerning organisation of the protection of state secrets.

(4) Requirements applicable to the responsible person or a structural unit, specified in subsection 2 of this section, shall be established by a regulation of the Government of the Republic under the procedure for protection of state secrets and classified information of foreign states.

(5) The head or a directing body of an agency, a constitutional institution, and a legal person in possession of state secrets is required to assign places of employment or posts where access to state secrets is a prerequisite for holding such post. Such posts are identified as a separate list or in the membership table, giving the required level of access to state secrets that is required for each post.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(6) The processing unit is required to establish the guidelines for the protection of classified information, laying down the requirements for the protection of state secrets and classified information of foreign states in the processing unit. The requirements for the guidelines are established by a regulation of the Government of the Republic under the procedure for protection of state secrets and classified information of foreign states.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(7) The possessor of a state secret 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 existence and integrity of media kept in archives must be inspected at least once every five years. Media covered by the obligation, types of media, classification level and the procedure for control thereof are established by a regulation of the Government of the Republic in accordance with the procedure for the protection of state secrets and classified foreign information.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(8) Upon termination of an agency, a constitutional institution, or a legal person in possession of state secrets, the classified media shall be deposited with the Internal Security Service or, in the case of the Defence League or the Defence Forces, a structural unit assigned by the Statutes of the Defence Forces.
[RT I 2008, 35, 213 – entry into force 01.01.2009]

§ 21. Use of weapon for protection of state secret

(1) A firearm 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.
[RT I, 29.06.2018, 3 – entry into force 01.07.2018]

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

§ 22. Competence of Internal Security Service and structural unit designated by statutes of Defence Forces in organising protection of state secrets

[RT I 2008, 35, 213 – entry into force 01.01.2009]

(1) The protection of state secrets shall be organised and supervision over implementation of this Act and any legislation established on the basis thereof shall be exercised by the Internal Security Service, and in the Defence Forces and the Defence League, by a structural unit designated under the statutes of the Defence Forces, except in the cases specified in § 23 of this Act.
[RT I 2008, 35, 213 – entry into force 01.01.2009]

(2) The Internal Security Service and a structural unit designated under the statutes of the Defence Forces are required, as appropriate, to:
[RT I 2008, 35, 213 – entry into force 01.01.2009]
1) supervise the compliance with the requirements of state secret protection in agencies, constitutional institutions and legal persons in possession of state secrets, and supervise the 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 any 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 the deficiencies and violations;
5) organise periodic training on issues of the protection of state secrets;
6) based on the risk assessment, check for the presence of illegal intercept devices in the security area of the processing unit.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(3) In the course of exercising supervision, the Internal Security Service and a structural unit designated under the statutes of the Defence Forces have the right to access all the necessary information and to issue precepts to the processing unit and a natural person with the right of access for the elimination of a violation or risk of violation of the requirements arising from this Act or any legislation issued on the basis thereof.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(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 Internal Security Service and a structural unit designated by the statutes of the Defence Forces, shall have the right to issue a mandatory precept to the possessor of state secrets for the suspension of the processing of state secrets and classified media and, if necessary, to take the classified media temporarily into storage until establishment of the necessary conditions.
[RT I 2008, 35, 213 – entry into force 01.01.2009]

(5) Upon failure to comply with the precept, specified in subsections 3 and 4 of this section, the Internal Security Service and a structural unit designated under the statutes of the Defence Forces shall have a right to apply substitutional performance and non-compliance levy in the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act and impose a non-compliance levy with a maximum value of 3,200 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

(5^1) Director General of the Internal Security Service approves the working schedule for the conduct of inspection of state secret protection by the Internal Security Service.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(6) The minister in charge of the policy sector approves the working procedure of the committee formed for the conduct of inspection of state secret protection by the Internal Security Service.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

§ 23. Competence of Estonian Foreign Intelligence Service in organising protection of state secrets

[RT I, 05.05.2017, 1 – entry into force 01.07.2017]

(1) The Estonian Foreign Intelligence Service:
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]
1) organise and verify compliance with the requirements established for INFOSEC;
2) organise and verify the protection of state secrets on foreign missions.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(2) The Estonian Foreign Intelligence Service shall, for the purpose of organisation and verification of INFOSEC:
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]
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 conformity certificate given to a processing system and a temporary permit of use;
5) co-operate with foreign states and international organisations in the sphere of INFOSEC;
6) organise and verify the processing of encrypted materials that are used to protect state secrets and the ensuring of radiation safety of processing systems, and provide advice and guidance therefor;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
7) applies security measures to protect the processing system in the case of a security failure or a threat thereof;
8) organise periodic training for assuring conformity with the INFOSEC requirements.

(3) On foreign missions the Estonian Foreign Intelligence Service:
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
1) supervise the compliance with the requirements of state secret protection and access by natural persons to state secrets;
2) supervise compliance with the 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 elimination of deficiencies and prevention of violations;
5) organise periodic training in order to ensure the compliance with the requirements of the protection of state secrets;
6) based on the risk assessment, check for the presence of illegal intercept devices in the security area of the processing unit.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(4) In the course of exercising supervision, the Estonian Foreign Intelligence Service shall have the right to access 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.
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]

(5) In the event that 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 Estonian Foreign Intelligence Service has the right to issue a precept to the processing unit or a natural person with the right of access to state secrets for the suspension of the processing of state secrets and classified media and, where necessary, to take the classified media or a part of a processing system temporarily into storage until establishment of the necessary conditions.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(6) Upon a failure to comply with the precept, specified in subsections 4 and 5 of this section the Estonian Foreign Intelligence Services hall have the right to apply substitutional performance and non-compliance levy in the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act. The maximum amount of the penalty fine to be imposed is 3,200 euros.
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]

§ 24. Competence of Security Committee of Government of Republic in organising 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 the minister and shall inform the Government of the Republic of the results of the review;
[RT I, 08.07.2011, 8 – entry into force 22.07.2011]
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 change of the grounds, level and term of classification.

Division 2
Access to state secrets

Subdivision 1
General provisions

§ 25. Granting access to state secrets

(1) The processing unit and the natural person with the right of access are required to verify before granting access to a state secret, whether the person holds the right of access to state secrets of the corresponding classification and whether the person has a need to know.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(2) If the 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 the right of access and need to know. Access is denied to the part of the medium that provides the basis for drawing conclusions on the part of the medium to which the person holds no right of 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) in case the processing unit needs to grant that person access in connection with the functions to be discharged by the processing unit and the person concerned has the required special knowledge, skills or equipment to contribute to discharging the aforementioned functions, or
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
3) in cases specified in §§ 29 or 30 of this Act.

Subdivision 2
Right of access

§ 26. Right of access to state secrets

(1) A person shall have the right of 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;
6) under the decision of the agency which performs security vetting.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(2) The right of access to a higher classification of state secrets shall also grant the right of access to a lower classification of state secrets. The right of access to a lower classification of state secrets shall not grant the right to access a higher classification of state secrets.

(3) The right of 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 facility security clearance shall not grant the right of access to state secrets to the person under contractual or service relationship with the person holding a facility security clearance.

(5) The term of the right of access granted in case of a temporary need for access, shall not exceed the term of the person's participation in the temporary task or work.

(6) The expiry of the right of access to state secrets shall not relieve the person who held the right of access from the obligation to maintain the confidentiality of a state secret.

(7) Upon expiry of the right of access the person who held the right of access must return all the classified media in their possession to the processing unit that granted the access to state secrets to the person. The media that contain state secrets created by the person who held the right of access are handed over to the processing unit that initiated the creation of information and to the Internal Security Service in all other cases.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

§ 27. Right of access to state secrets by virtue of office and under decision of head of agency

(1) The right of access to any level of state secret is, under this Act, given by virtue of office to the following individuals:
1) the President of the Republic;
2) a member of the Riigikogu;
3) a member of the Government of the Republic;
4) a judge;
5) the Commander of the Defence Forces;
[RT I, 08.07.2011, 8 – entry into force 22.07.2011]
6) the Chancellor of Justice and the Deputy Chancellor of Justice-Adviser;
7) the Auditor General;
8) the Governor of Eesti Pank, Chairman and member of the Executive Board of Eesti Pank;
9) the Head of the Estonian Data Protection Inspectorate.
[RT I, 08.07.2011, 8 – entry into force 18.11.2010]

(2) The right of access only to state secrets classified as 'restricted' is granted, by virtue of office, to a natural person who is appointed, elected, or hired under an employment contract to a place of employment or a post that requires the right of access to state secrets classified as 'restricted' as a prerequisite for employment in this post at a state authority, Eesti Pank or the Estonian Defence League.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(3) If circumstances specified in subsection 1 of § 32 of this Act are revealed concerning the person applying for or holding the post specified in subsection 2 of this section:
1) this person shall not be given a post that requires access to state secrets; or
2) this person is dismissed from the post 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 employment contract, signed with this person, is terminated, as provided for in the Employment Contracts Act of the Republic of Estonia.
[RT I 2009, 5, 35 – entry into force 01.07.2009]

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

(5) The decision to grant natural persons outside the services the right of access only to a state secret classified as 'restricted', is adopted separately in each case by:
[RT I, 08.07.2011, 8 – entry into force 18.11.2010]
1) appropriate minister or the head of an authority within the area of government of the ministry with the authorisation of the minister, or the Commander of the Estonian Defence League;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
2) the head of the appropriate institution in the case of the Chancellery of the Riigikogu, the Office of the President, the Government Office, the Office of the Chancellor of Justice, the Eesti Pank, courts, the State Audit Office and a security authority
3) the Governor of Eesti Pank in the Financial Supervision Authority.

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

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

(8) If circumstances specified in subsection 2 of § 32 of this Act are revealed regarding the person specified in subsection 5 of this section, the head of a security authority that conducts the security vetting on the person, may deprive the person of the right of access to state secrets classified as 'restricted' or prohibit the granting of 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 of access and a notice regarding the adoption of such decision to an agency, constitutional institution or a legal person which employs the person or which granted the right of access to the person concerned.

(10) If a person applying for or holding the right of access only to a state secret classified as 'restricted' holds no right of 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, the 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 a security vetting to obtain 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 of access or extending its term as well as during the validity of the right of access.

(11) The verification and consent specified in subsection 10 of this section and a copy of the resolution adopted under subsection 5 of this section shall be sent to the agency competent to conduct the security vetting concerning the person.
[RT I, 08.11.2010 – entry into force 18.11.2010]

(12) Should the person refuse to give the verification or consent, specified in subsection 10 of this section, the person shall not be granted the right of access only to state secrets classified as 'restricted'. Subsection 3 of this section shall be applicable in this case to a person who applies for or holds an office requiring the right of access to state secrets classified as 'restricted'.

(13) The format of the documents specified in clauses 2 and 3 of subsection 10 of this section shall be established by a regulation of the Government of the Republic under the Procedure for Protection of State Secrets and Classified Information of Foreign States.

§ 28. Right of access to state secrets under Personnel Security Clearance

(1) The right of access to state secrets classified as 'confidential', 'secret' or 'top secret' is available to a natural person who has been granted a Personnel Security Clearance to state secrets (hereinafter a personnel security clearance) of an appropriate level.

(2) If provided for under an international agreement, application for the Personnel Security Clearance shall not be required from a citizen of a foreign state or a person with no citizenship who is holding the right of access to the appropriate level of classified information of a foreign state.

§ 29. Right of access to state secret on basis of reasoned order of investigative body or prosecutor's office or court ruling

(1) Participants in pre-trial proceedings or judicial proceedings, an individual involved in the proceedings and the representatives of both parties in criminal, civil or administrative matters, or matters of misdemeanour shall have the right to access, after passing the security vetting, state secrets classified as "restricted", "confidential"

or “secret” on the basis of a reasoned order of an investigative body, the 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.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(2) Access on the basis of a reasoned order from an investigative body, the Prosecutor’s office or a court ruling shall not be permitted to state secrets classified as “restricted”, “confidential” or “secret” if this endangers the protection of rights provided for in clauses 2, 4, 5, 6, and 7 of § 126^{14} of the Code of Criminal Procedure, and to state secrets classified as “top secret”.
[RT I, 21.06.2014, 11 – entry into force 01.07.2014]

(3) A security vetting shall not be performed in respect of suspects, the accused at trial and a counsel who is an advocate if the need to know arises from ensuring the right of defence in criminal proceedings.

(4) An investigative body, the Prosecutor’s office or a court shall forward an application for the conduct of a security vetting to an agency which performs a security vetting in order to decide on the granting of the right to access state secrets to a person. In order to pass the security vetting, the person shall submit the document specified in clause 3 of subsection 10 of § 27 of this Act to the agency which performs a security vetting.

(5) The agency which performs a security vetting shall present the information obtained as a result of a security vetting to an investigative body, the Prosecutor’s office or a court within the term specified thereby, and this term shall not be less than one month.

(6) An investigative body, the Prosecutor’s office who prepared an order or a court which prepared a ruling shall notify the person to be granted a right of 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 verification specified in clause 2 of subsection 10 of § 27 of this Act from a person before access to the information is granted, which shall be included in the materials of the file.

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

§ 30. Right of access to state secrets of persons protected under 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 to access state secrets concerning his or her protection without a Personnel Security Clearance or compliance with the requirement to pass a 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 verification, specified in clause 2 of subsection 10 of § 27 of this Act. The person refusing to give the verification shall not be granted the right of access to state secrets.

(2) A representative of the person specified in subsection 1 of this section, not being a lawyer, is given access to state secrets concerning the protection of the aforementioned person after passing a security vetting to the extent that is deemed necessary. Subsections 4–7 of § 29 of this Act are applicable to such cases.

§ 30^{1}. Right of access to state secrets based on decision of agency which performs security vetting

(1) The right of access to the state secrets of confidential national defence and infrastructure and information protection after passing security vetting is the right of access of a person liable to national defence obligation appointed to a wartime position of military rank (wartime post), where access is unavoidably necessary for the performance of the duties of their position.

(2) A request to perform a security vetting on the person specified in subsection 1 of this section and grant the person the right of access is submitted by the Defence Forces to the agency which performs the security vetting.

(3) The Defence Forces inform the person specified in subsection 1 of this section of the intention to submit a request to perform a security vetting on the person and grant the person the right of access, and set a time-limit, which may not be shorter than ten working days, during which the person has the right to refuse security vetting in a form reproducible in writing.

(4) In case the person has not refused the security vetting within the time limit specified in subsection 3 of this section, the Defence Forces forward to the authority, which performs security vetting, a request to perform a security vetting and grant the right of access.

(5) During increased defence readiness, an emergency situation, mobilization and a state of war, and in the event of an invitation to an additional reservist training, a security vetting may be carried out on the person specified in subsection 1 of this section without the consent of the person.

(6) The agency which performs security vetting decides whether to grant the right of access.

(7) The right of access is granted for up to five years and is valid only during the performance of the duties of a wartime position of military rank.

(8) In case the circumstance specified in subsection 1 of § 32 of this Act exists for the person specified in subsection 1 of this section, the person is not granted the right of access or is deprived of the right of access already granted.

(9) In case the circumstance specified in subsection 2 of § 32 of this Act appears for the person specified in subsection 1 of this section, the person may be refused the right of access, or the right of access already granted may be revoked.

(10) The agency which performs security vetting has the right to ask the person specified in subsection 1 of this section and the Defence Forces for additional information to perform a security vetting. The person may refuse to provide it.

(11) The security vetting regarding the person specified in subsection 1 of this section is carried out at the latest by the time of entry into the military service. The agency which performs security vetting may, in justified cases, extend the term of the security vetting, notifying the Defence Forces thereof.

(12) The agency which has performed the security vetting immediately notifies the Defence Forces of the granting, refusal to grant or deprivation of the right of access.

(13) The Defence Forces notify the person specified in subsection 1 of this section of the granting of the right of access, refusal to grant or the expiry of the right of access.

(14) The Defence Forces immediately inform the agency that has performed the security vetting of the lapse of the need for access by the person specified in subsection 1 of this section.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

Subdivision 3
Application for issue, issue, extension of term and expiry of Personnel Security Clearance

§ 31. Application for Personnel Security Clearance or extension of term thereof

(1) In order to obtain a Personnel Security Clearance (hereinafter the PSC) or to be granted extension of the term thereof, a person submits a request to the competent authority to carry out security vetting on themselves, through a constitutional institution, government authority or state authority administrated by a government authority (hereinafter the 'sponsor of a PSC') supporting the granting of a PSC or extension of the term thereof, or in the respective electronic environment, to which the following documents are appended:
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
1) a letter from the sponsor of the PSC (except if the sponsor of the PSC and the agency performing a 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 granting of the PSC or extension of the term thereof;
2) a completed form by the applicant for a PSC upon application for and extension of the PSC;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
3) documents specified in clauses 2 and 3 of subsection 10 of § 27 of this Act.

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

(3) In order to be granted extension of the term of a PSC, the documents required for extension shall be submitted to the agency that performs a security vetting no later than three months before the expiry of the PSC.

(4) In the case of the timely submission of the documents required for the grant of extension of the term of a PSC, the term of the PSC shall be extended until the decision to extend or refuse from reviewing the application has been adopted.

(5) The format of the application for a PSC or extension of the term thereof and the format of an application form of a person applying for a PSC or extension thereof shall be established by a Regulation of the Government of the Republic under the Procedure for Protection of State Secrets and Classified Information of Foreign States.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

§ 32. Bases for refusal to grant Personnel Security Clearance or extend term thereof

(1) A PSC shall not be granted or extension of the term thereof shall be refused to a natural person:
1) with no need for access;
2) who is not in compliance with the requirements provided for in subsection 1 of § 33 of this Act;
3) with restricted active legal capacity;
4) who is employed or has been employed by the intelligence or security service of a foreign state, except if the person complies with the requirements provided for in subsection 3 of § 25 of this Act and, according to a security authority assessment, does not pose a threat to the security of the Republic of Estonia;
5) who has been disclosed or is 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 is serving a prison sentence;
7) whose activities are directed against the Republic of Estonia state and its national security;
8) who has been punished for committing intentionally an offence against the state or humanity regardless of whether or not the data on punishment have been expunged from the criminal records database;
9) who has been deprived of the right of access due to violation of the provisions of this Act or legislation issued on the basis thereof;
10) whose previously granted PSC has been revoked due to violation of the provisions of the State Secrets Act or legislation issued on the basis thereof within the period of five years as of the revocation of the PSC.

(2) The granting of a PSC or extension of the term thereof may be refused to a natural person:
1) whose activities have been directed against the Republic of Estonia and its national security;
1^1) who has been involved in co-operation with an intelligence or security service of a foreign state;
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]
2) who is involved with a person or an organisation which by its activities ignores public policy or the purpose of which is to change the autonomy and 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;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
3) who is participant in criminal proceedings as a suspect or accused;
4) who has several punishment for misdemeanours and the information concerning the punishment has not been expunged from the criminal records database;
5) who has been punished for intentionally committed official misdemeanour or criminal official misconduct that the person has committed as an official, regardless of whether or not the information concerning punishment has been expunged from the criminal records database, or with regard to whom the proceedings commenced for criminal official misconduct or criminal offences against the state have been dropped under §§ 202, 203, 205 or $205^2$of the Code of Criminal Procedure;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
6) against whom misdemeanour proceedings are conducted with comprising elements of criminal official misconduct or acts of corruption or violation of this Act or any legislation issued on the basis thereof;
7) who has been punished for an intentionally committed criminal offence and the information concerning the punishment has not been expunged from the criminal records database;
8) who has been punished for committing a criminal offence against the state due to negligence, regardless of whether or not the information concerning the punishment has been expunged from the criminal records database;
9) who is or has been diagnosed with dependence on narcotic or psychotropic drugs, alcohol or gambling;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
10) who has intentionally concealed information, submitted false or falsified information that is essential in deciding the grant of a PSC in the application form for a PSC or for extension of the term thereof submitted to the agency that performs a security vetting or in the interview for applicants for a PSC;
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]
11) who has not performed all of his or her obligations regarding state and local taxes;
12) who has stayed in a foreign state for a longer period under circumstances that cannot be identified;
12^1) who has stayed in a foreign state for which a notification requirement is applied under the circumstances that cannot be identified;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
13) who suffers from mental disturbances that limit his or her ability to understand or control his or her behaviour;
14) who is socially or economically dependent on a person with respect to whom a fact specified in clauses 4, 5 or 7 of subsection 1, or in clause 1, 1^1, 2 or 8 of subsection 2 of this section exists;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
15) who has, either by word or act, expressed dishonesty, disloyalty, unreliability or indiscretion that may refer to the person's unreliability upon maintenance of a state secret;
16) who indulges a well-developed pattern of behaviour or addiction, which may result in economic dependence of the person;
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

17) who has not complied with the notification requirement provided for in subsection 2 of § 19 of this Act;
[RT I, 06.03.2015, 9 – entry into force. 16.03.2015]
18) who has been explained, on the basis of subsection 5 of § 19 of this Act, the threat to the national security related to the travelling to a foreign state but who has not followed the recommendations given thereto related to the travelling to or staying in a foreign state for the prevention of the attempts of unlawful access to state secrets.
[RT I, 06.03.2015, 9 – entry into force. 16.03.2015]
19) whose behaviour may entail the risk of becoming the object of blackmail or other pressure;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
20) who has repeatedly violated the requirements for the protection of state secrets or classified information of foreign states or has disregarded the obligation provided in subsection 1 or 2 of § 19 of this Act.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(3) A security vetting shall be performed with regard to a person in the procedure provided for in this Act to check the facts specified in subsections 1 and 2 of this section.

(4) If the facts specified in subsections 1 or 2 of this section become evident in respect of a person, the agency, constitutional institution and legal body which is in employment or contractual relationships with the person is required to immediately notify thereof the agency competent to perform a security vetting with respect to the person.

§ 33. Granting of Personnel Security Clearance and extension of term thereof

(1) A Personnel Security Clearance (PSC) may be granted to a citizen of Estonia, or a natural person specified in subsection 3 of § 25 of this Act.

(2) The basis for the granting of, refusal to grant, extension of the term and revocation of a PSC is a decision which is made based on the information gathered in the course of the security clearance.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(3) The decision on the granting of a PSC, refusal to grant, extension of the term or revocation of the validity is made by the head of the agency which conducted the security vetting at the latest within three months as of the submission of the documents required for the granting of a PSC or extension of its term. A PSC is granted by an agency that has conducted a security vetting with respect to the person.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(4) An agency which performs a security vetting may extend the term provided for 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 PSC in the course of a security vetting within the period of three months as of the submission of the required documents due to material circumstances depending on the applicant;
1^1) where it has not been possible to conduct an interview with the applicant for a PSC in the course of a security vetting within the period of three months as of the proper submission of the documents due to an emergency situation, a state of emergency, increased defence readiness or a state of war;
[RT I, 06.05.2020, 1 – entry into force 07.05.2020]
2) where it is necessary for the decision on the granting of a PSC to be based on information originating from a foreign state;
3) where information gathered in the course of a security vetting indicates that bases for refusal to grant a PSC are likely to become evident within the following three months;
4) where information gathered in the course of a security vetting indicates that bases for refusal to grant a PSC may cease to exist in respect of the person subject to a security vetting within the following three months.

(5) An agency which performs a 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 PSC in the course of a 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 the right of 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 a PSC or his or her sponsor;
4) under other circumstances provided by law.

(6) If a PSC to the classification level of state secrets specified in the application cannot be granted to a person or extension of the term thereof is not possible as a result of the consideration of circumstances specified in subsection 2 of § 32 of this Act but it would be possible to grant a PSC or extend the term thereof to a lower level of classification, a PSC or extension of the term thereof is granted for a lower level of classification, if considered necessary by the applicant for the permit and his or her sponsor.

(7) In order to access state secrets classified as ‘top secret’ or ‘secret’, a PSC shall be granted 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 PSC shall be granted to a person for up to seven years or the term thereof shall be extended for up to seven years.

(8) In case the granting of a PSC is applied for by a person who wishes to assume a place of employment or post where access to state secrets is a prerequisite for the performance of tasks or who wants to enter into an agreement where access to state secrets is a prerequisite for the performance of the agreement, the granted PSC is validated as of the moment for the appointment or assignation of the person to the post or as of the enforcement of the appropriate provision of the contract. The term of the PSC is then calculated as of the date of the granting of a PSC.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(9) The PSC or a notice concerning extension of the term of validity thereof must set out the following data:
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
1) the date of the granting a PSC or extension of the term thereof and the number of the decision;
2) the basis for the decision;
3) the given name, surname and the personal identification code of the person;
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]
4) the classification of state secrets which the person is permitted to access;
5) the term of a PSC.

(10) Upon granting the PSC or extension of the term thereof, a notice is sent through the sponsor of the PSC or in the respective electronic environment to the applicant for the PSC within five working days as of the adoption of the decision.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(11) Upon refusal to grant a PSC or extend the term thereof, the agency which performs a security vetting shall send an officially certified copy of the decision to refuse to grant a PSC or extend the term thereof to the applicant for a PSC and the notification about the decision to refuse the granting of a PSC to the agency which justifies the need for access and supports the granting of a PSC within five working days, except if the agency that supports the granting of a PSC is the agency performing a security vetting.

(12) In case a person is holding a place of employment or a post where access to state secrets is a prerequisite for the performance of tasks, or is applying for such post, and the person is refused the granting of a PSC or the extension of the term thereof, provisions of clauses 1 and 2 of subsection 3 of §27 of this Act apply.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

§ 34. Expiry of Personnel Security Clearance

(1) A PSC shall expire:
1) upon the death of a person, a person being declared dead or going missing;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
2) upon expiry of the term specified in a PSC;
3) upon revocation of a PSC;
4) upon revocation of the right of access of a person with an enforced court ruling or the decision of a body conducting extrajudicial proceedings.

(2) A PSC that has been granted to a person is declared invalid if circumstances specified in subsection 1 of § 32 of this Act become evident with respect to that person.

(3) A PSC that has been granted to a person may be declared invalid if circumstances specified in subsection 2 of § 32 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 PSC need not be revoked.

(5) The agency that has the capacity to decide on the extension of the term of a PSC that has been granted to the person shall revoke a PSC.

(6) The sponsor of granting of a PSC and an agency, constitutional institution, or legal body, in which a natural person whose PSC is revoked is employed or contracted by, shall promptly be notified of the revocation or repeal of the PSC of the natural person. Notification of the revocation of the PSC is not required if the sponsor of the granting of a PSC and an agency, constitutional institution, or legal body, in which a natural person whose PSC is revoked is employed or contracted by, requested the revocation of the PSC on the bases of clause 1 of subsection 1 of § 32 upon the expiry of employment or contractual relationship.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(7) The agency which performs a security vetting shall immediately inform the Estonian National Security Authority (hereinafter the National Security Authority) of the expiry of the term of a PSC of a person holding a PSC on the basis of clauses 3 of 4 of subsection 1 of this section.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(8) In case a person who holds a place of employment or a post where access to state secrets is a prerequisite for the performance of the tasks, or is applying for such post, is refused the granting of a PSC or the extension of the term thereof or the PSC is declared void or its invalidity is identified, the provisions of subsection 3 of §27 of this Act apply.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

Division 3
Processing of state secrets and classified media

Subdivision 1
General provisions

§ 35. Communication of state secrets

(1) Internally, state secrets communicated to a holder of classified information may only be communicated with the written consent of a head or directing body of an agency, constitutional institution, or public legal person that is the originator of the state secret or, in the case of a state secret related to criminal proceedings, of 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. In case a natural person outside a service or a legal person governed by private law is an originator of the information, the constitutional institution, government authority or state agency governed by the government authority grants the written consent for communication of information which was created for compliance with the contract entered into.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(2) 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 granting of a Personnel Security Clearance or a Facility Security Clearance has ceased to exist, the consent for communication is given by the minister in charge of the policy sector.

(3) 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, the National Security Authority, a court, the Riigikogu, the Chancellor of Justice, the Auditor General, the Government of the Republic and, in the case provided for in subsection 2 of § 10 of the Security Authorities Act, to relevant governmental authorities and the President of the Republic.
[RT I, 12.03.2015, 1 – entry into force 01.01.2016]

(4) State secrets may be communicated to a foreign state, international organisation or an institution established under an international agreement by the holder of information in accordance with the rules provided in this Act and legislation issued on the basis thereof:
1) based on a treaty, or
2) based on the decision of the Security Committee of the Government of the Republic in case the recipient of information ensures the protection of the communicated information from disclosure.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(5) State secrets may be communicated to a foreign state, international organisation, or an institution established under an international agreement by the Police and Border Guard Board, observing the procedure specified in this Act and legislation issued on the basis thereof and the provisions of the Witness Protection Act, provided that the agency receiving the information shall ensure the protection of communicated information from disclosure.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(5^1) State secrets containing surveillance information at the ‘restricted’ level that is required for the maintenance of law and order may be communicated to a foreign state, international organisation, or an institution established under an international agreement by a competent surveillance authority or the Prosecutor’s Office if such obligation is due under the European Union law or an international agreement or is required for the work of an international investigation group, provided that the agency receiving the information shall ensure the protection of the communicated information from disclosure.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(6) Communication of state secrets to a foreign state, international organisation or an institution established under an international agreement is first registered at the National Security Authority, except in case:
1) information is communicated by a security authority;
2) information specified in clauses 5^1, 7, 10 and 11 of § 7 of this Act is communicated by the Defence Forces;
3) information about witness protection is communicated by the Police and Border Guard Board;
4) information classified as “restricted” specified in clauses 1–3 of § 8 of this Act is communicated by the surveillance agency or the Prosecutor's Office.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

§ 36. Registration of classified information

[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(1) Registration of classified media is performed based on the Administrative Procedure Act and the Archives Act and the legislation issued based on them, taking into account the special rules provided in this Act and the legislation issued on the basis thereof.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(2) Registration of copies made of classified media, except the 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 for Protection of State Secrets and Classified Information of Foreign States.

§ 37. Marking of classified media

(1) Classified media must be marked, taking into account their type and characteristics, in a manner that allows:
1) their holder to understand that it is classified information;
2) their processor to find out the level and term of classification of information, legal basis, as well as information about additional security measures and the circle of persons who have the right of access to the medium in case they have been determined.
[RT I, 07.03.2023, 7 – enters into force. 01.04.2023]

(2) A classified medium may be left unmarked in case, due to the marking, there may arise a risk for the classification of a state secret, or marking is not possible due to the type or characteristics of the medium.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(3) [Repealed – RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(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 so provided by an international agreement.

(5) [Repealed – RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(6) [Repealed – RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(7) Upon declassification of information recorded on a classified medium, the holder of the medium is obliged to change the relevant marking in a manner that enables the holder of the medium to understand that it is no longer classified information.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

§ 38. Storage and destruction of classified media

(1) Archival information is transferred after the expiry of classification to the National Archives in accordance with the Archives Act.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(2) The part of medium containing a special category of personal data, collected as a result of the collection of information of surveillance activities, is not transferred to the National Archives in case the person regarding whom the surveillance activities were conducted, or whose private or family life was violated by the surveillance activities, requests the destruction of information containing a special category of personal data and this information is no longer required for performance of public tasks. In such cases, the part of medium that contains a special category of personal data is destroyed in a manner that make impossible the restoring of the information contained therein.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(3) In the case of the media where the classification of information entered into has not expired, it is only allowed to destroy:
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
1) a copy made of classified media;
2) a classified medium in an unexpected situation where there is no other alternative available to protect the medium from access by a person not having the right of 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, the Internal Security Service and the Security Committee of the Government of the Republic of Estonia shall be promptly notified of the destruction and the reasons thereof;

3) a draft after the compilation of a medium that the draft was prepared for;
4) a classified medium which contains only information without archival value;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
4[1]) a classified medium, the information of archival value contained in which has been transferred to another medium in a manner that ensures its authenticity, reliability, integrity and usability;
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]
5) [Repealed – RT I, 07.03.2023, 7 – entry into force 01.04.2023]
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 more specific requirements for processing state secrets and classified media shall be established by a regulation of the Government of the Republic under the Procedure of Protection of State Secrets and Classified Information of Foreign States, including:
1) elektroonilise teabeturbe nõuded, sealhulgas töötlussüsteemile esitatavad nõuded, välja arvatud käesoleva paragrahvi lõikes 2 sätestatud nõuded;
[RT I, 07.03.2023, 7 – jõust. 01.01.2024]
2) requirements for processing state secrets outside the security area.
[RT I, 06.03.2015, 9 – entry into force 16.03.2015]

(2) The minister in charge of the policy sector shall adopt a regulation, specifying the following, for INFOSEC purposes:
1) requirements to encrypted materials and processing and protection thereof;
2) requirements for ensuring radiation safety
3) [repealed – RT I, 07.03.2023, 7 – entry into force 01.01.2024]

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

Subdivision 2
Admissibility to processing of state secrets

§ 40. Admissibility to Processing of State Secrets

(1) (1) State secrets and classified media may be processed on the immovable or movable held by a state authority, the Estonian Defence League or Eesti Pank, unless otherwise provided in this Act or legislation issued on the basis thereof.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(2) With the appropriate permit issued by the Internal Security Service (hereinafter referred to as the 'Facility Security Clearance'), state secrets and media containing thereof may also be processed outside the immovable and movable held by a state authority, the Estonian Defence League or Eesti Pank, provided that the person has a justified need therefor.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(3) A Facility Security Clearance may be granted 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 processing classified information in its branch, registered in Estonia, for the participation of a person in negotiations concerning a public or international procurement or if the agency which possesses state secrets needs to permit access by such persons to the state secrets in connection with the functions imposed on the agency and if the person has the necessary special knowledge or skills or means to assist in the performance of such functions.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(4) A Facility Security Clearance is granted to a legal person only after the person organising the protection of state secrets within the legal person has been issued a Personnel Security Clearance.

(5) The processing system may only be used for the processing of state secrets if a conformity certificate or a temporary permit of use, issued by the Estonian Foreign Intelligence Service, is available.
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]

§ 41. Application for Facility Security Clearance or extension of term thereof

(1) In order to obtain a Facility Security Clearance or to be granted extension of the term thereof, a person submits an application which justifies the need for processing and supports the receipt of the Facility Security Clearance or extension of the term thereof to the Internal Security Service through a constitutional institution, government authority or state agency governed by a government authority (hereinafter the 'sponsor of a Facility Security Clearance), or in a respective electronic environment, to which the following documents are annexed:
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
1) a letter from the sponsor of the Facility Security Clearance, which sets out the type or types of state secret for the processing of which the Facility Security Clearance is requested, with a reference to the basis of the classification of information and justifies the need of a person in the service or contractual relationship or requesting thereof to process state secrets and classified media containing thereof outside the immovable and movable held by a state authority, the Estonian Defence League or Eesti Pank, and sponsor the granting of the Facility Security Clearance or the extension of the term thereof;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
2) a document that proves the right of 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 the right of access was granted by the Internal Security Service;
3) the documents specified in clauses 2 and 3 of subsection 10 of § 27 of this Act in the case of a legal person and a completed form of natural persons upon application for a Facility Security Clearance or, upon extension of the term of a Facility Security Clearance, a completed annex to the form.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

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

(3) In order to be granted extension of the term of a Facility Security Clearance, an application together with the documents appended thereto shall be submitted to the Internal Security Service not later than three months before the expiry of the Facility Security Clearance. Natural persons and legal persons are required to submit an application to the supporting agency no later than four months and seven months before the expiry of the Facility Security Clearance, respectively.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(4) The term of a Facility 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 for granting an extension of the term of a Facility Security Clearance.

(5) The application specified in subsections 1 or 2 of this section may be submitted together with the application for a Personnel Security Clearance or the extension of the term thereof.

(6) The format of the application for a Facility 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, adopted under the Procedure for Protection of State Secrets and Classified Information of Foreign States.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

§ 42. Bases for refusal to grant Facility Security Clearance or extend term thereof

(1) A Facility Security Clearance shall not be granted to or an extension of the term thereof shall be refused to natural persons:
1) who lack the right of access;
2) who lack a justified need to process a state secret or classified media containing thereof outside the immovable and movable held by a state authority, the Estonian Defence League or Eesti Pank;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
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 the processing rights.

(2) A Facility Security Clearance shall not be granted to or an extension of the term thereof shall be refused to legal persons:
1) who lack the need for access;
2) with respect to whom the circumstances specified in clauses 2–4 of subsection 1 of this section exist;
3) who do not meet the requirements, specified in subsections 3 or 4 of § 40 of this Act;
4) with respect to whom the circumstances specified in clauses 7, 8 or 10 of subsection 1 of § 32 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 a liquidation procedure.

(3) The granting of a Facility Security Clearance or extension of the term thereof may be refused to legal persons:
1) with respect to whom the circumstances specified in clauses 1–8, 10 or 11 of subsection 2 of § 32 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, violated any public procurement contracts;
4) at least one third of the shareholders or participation of which belongs to a person that cannot be identified.

(4) The procedure for checking the existence of circumstances specified in clause 3 of subsection 1 of this section shall be established by a regulation of the Government of the Republic, adopted under the Procedure of Protection of State Secrets and Classified Information of Foreign States.

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

(6) An agency, a constitutional institution, and a legal body in which the person is employed under service or contractual relationship is required to notify the Internal Security Service of persons in respect of whom the circumstances provided for in subsections 1, 2 and 3 of this section become evident.

§ 43. Granting of Facility Security Clearance and extension of term thereof

(1) The basis for the granting of a Facility Security Clearance or extension of the term thereof is information gathered for verification of the fact specified in clause 3 of subsection 1 of § 42 of this Act.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(2) The basis for the granting of a Facility Security Clearance to a legal person or extension of the term thereof is also, in addition to the information specified in subsection 1 of this section, information gathered in the course of the security vetting.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(3) The granting of a Facility Security Clearance or extension of the term thereof shall be decided no later than within two months in the case of natural persons and no later than within six months in the case of legal persons, after the submission of a valid application. In cases specified in subsection 5 of § 41 of this Act, the granting of a Facility Security Clearance or extension of the term thereof shall be decided immediately after the granting 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 Facility Security Clearance 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 Facility Security Clearance within six months in the course of a security vetting due to material circumstances depending on the applicant;
3) where information gathered about the legal person applying for a Facility Security Clearance in the course of the security vetting indicates that bases for refusal to grant a Facility Security Clearance are likely to become evident within the following six months;
4) where information gathered in the course of a security vetting indicates that bases for refusal to grant a Facility Security Clearance may cease to exist in respect of the legal person applying for a Facility Security Clearance and subject to a security vetting within the following six months.

(5) The Internal Security Service shall refuse to review the application in the following cases:
1) the granting of a Facility Security Clearance 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 a Facility Security Clearance or a sponsor of a Facility Security Clearance to refuse the review of the application;
3) where it has not been possible to conduct an interview with the representative of the legal person applicant for a Facility Security Clearance in the course of a 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 circumstances provided by law.

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

(7) A Facility Security Clearance is issued or the term thereof is extended for a fixed term in case the need to process a state secret or media containing classified information outside the immovable and movable held by a

state authority, the Estonian Defence League or Eesti Pank is of a temporary nature, but in the case of a natural person applicant the term is not extended for longer than the term of the expiry of the right of access to the state secret.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(8) A Facility Security Clearance or a notice concerning extension of the term thereof must set out the following data:
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]
1) the date of the granting of a Facility Security Clearance or extension of the term thereof and the number of the decision;
[RT I, 06.03.2015, 9 – entry into force 16.03.2015]
2) the basis and justification for the granting of a Facility Security Clearance or extension of the term thereof;
3) the given name, surname, personal identification code and a job or post of the person if a Facility Security Clearance is granted to a natural person;
4) name, seat and registry code of the person if a Facility Security Clearance is issued to a legal person;
5) the classification and level of state secrets which the person is permitted to process or only the level;
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]
6) the term of a Facility Security Clearance.

(9) A respective notice concerning the granting of a Facility Security Clearance, or the extension of the term thereof is sent by the Internal Security Service to the applicant for the Facility Security Clearance through the sponsor of the Facility Security Clearance or in the respective electronic environment, within five working days as of the adoption of the decision.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(10) Upon refusal to grant a Facility Security Clearance or to extend the term thereof, the Internal Security Service shall send within five working days an officially certified copy of the decision to refuse to grant a Facility Security Clearance or to extend the term thereof to the person who was denied the granting of a Facility Security Clearance or extension of the term thereof and a notice regarding the decision is sent to the sponsor of a Facility Security Clearance.

§ 44. Expiry of Facility Security Clearance

(1) A Facility Security Clearance shall expire:
1) upon the expiry of the right of 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 by an enforced court ruling or the decision of a body conducting extrajudicial proceedings;
4) upon expiry of the term specified in a Facility Security Clearance;
5) upon revocation of a Facility Security Clearance.

(2) A Facility Security Clearance shall be revoked if:
1) a person’s justified need to process a state secret or classified media containing thereof outside the immovable and movable held by a state authority, the Estonian Defence League or Eesti Pank has ceased to exist;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
2) the conditions provided by the person do not comply with the conditions required for the protection of state secrets and classified media, provided for by this Act and the legislation issued on the basis thereof;
3) the right of access to state secrets granted to a natural person has expired;
4) circumstances specified in subsection 2 of § 42 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 a state secret or classified media containing state secrets outside the immovable and movable held by a state authority, the Estonian Defence League or Eesti Pank, a Facility Security Clearance need not be revoked.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(4) A Facility Security Clearance granted to a legal person may be also revoked if:
1) circumstances specified in subsection 3 of § 42 of this Act exist with respect to the person;
2) the legal person is reorganised.

(5) A Facility Security Clearance shall be revoked by the Director General of the Internal Security Service. The Internal Security Service shall send within five working days an officially certified copy of the decision to revoke the permit to the person whose Facility Security Clearance was revoked and a notice regarding the decision to the sponsor of a Facility Security Clearance.

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

(7) The sponsor of a Facility Security Clearance and the head or the directing body of a legal person and the person who is authorized to organize protection of state secrets by the legal person whose Facility Security Clearance is revoked or identified as invalid, shall promptly be notified of the revocation of the Facility Security Clearance of the legal person.

(8) Upon the expiry or revocation of the Facility Security Clearance the person who has been granted the Facility Security Clearance returns all the classified media in their possession to the processing unit that granted the access to state secrets to the person. Media that contain state secrets created by the person who held the Facility Security Clearance are handed over to the processing unit that initiated the creation of information, and to the Internal Security Service in all other cases.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

§ 45. Obligations of Legal Person in Private Law who Holds Facility Security Clearance

A legal person in private law who holds a Facility Security Clearance is, in addition to compliance with the requirements specified in § 19 of this Act, required to notify the Internal Security Service promptly of the following circumstances:
1) a merger, division or reorganisation of a legal body;
2) the changing of members of the Management or Supervisory Board;
3) the contact information 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 per cent of equity or if the total value of material liability exceeds 70 per cent of equity;
5) bankruptcy or liquidation proceedings that have been initiated with respect to a legal person.

§ 46. Certificate of conformity of processing system and temporary use permit

(1) The Estonian Foreign Intelligence Service shall issue a certificate of conformity to a processing system as a result of accreditation, provided that the processing system complies with the INFOSEC requirements. The classification level of information that is permitted for processing by the system and the term of a certificate of conformity shall be specified in the certificate of conformity.
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]

(2) The Estonian Foreign Intelligence Service shall issue a Temporary Use Permit to a processing system as a result of accreditation if the processing systems do not comply with the INFOSEC requirements, but the related security risks are temporarily acceptable. The Temporary Use Permit shall specify the classification level of information that is permitted for processing by the system, the term of the Temporary Use Permit, and the obligation, conditions and term for new accreditation of the processing system.
[RT I, 05.05.2017, 1 – entry into force 01.07.2017]

(3) In case the electronic processing of a state secret takes place outside the immovable or movable held by a state authority, the Estonian Defence League or Eesti Pank, the granting of the certificate of conformity or a Temporary Use Permit 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.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(3) If electronic processing of state secrets takes place outside the immovable or movable possessed by a state agency or Eesti Pank, the issue of a certificate of conformity or a Temporary Use Permit 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 certificate of conformity to a processing system and temporary permit of use shall be established by a Regulation of the Government of the Republic under the Procedure for Protection of State Secrets and Classified Information of Foreign States.

Division 4
Security vetting

§ 47. Basis for performing security vetting

(1) The performance of a security vetting shall only mean the checking of the existence of circumstances specified in § 32 and subsections 2 and 3 of § 42 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 the right of access under a Personnel Security Clearance or based on an order of an investigative body, the Prosecutor's Office or a court order, or to obtain the Facility Security Clearance of a legal person or to be granted extension of the term of the right of access or the Facility Security Clearance, or to be granted the right of access provided in subsection 7 of § 30^1 of this Act, the applicant must pass a security vetting.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(3) The agency which performs security vetting is entitled to verify the existence of circumstances specified in § 32 and subsections 2 and 3 of § 42 of this Act also during the period of validity of the Personnel Security Clearance and the Facility Security Clearance of a legal person and during the period of validity of the right of access provided in subsection 7 of § 30^1 of this Act within the period of five years as of the expiry of the term in case the person, during the term of validity of the Personnel Security Clearance, has come across classified information which, once disclosed, would considerably damage national security.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(4) If there is a justified suspicion that circumstances providing the grounds for refusal to grant the Personnel Security Clearance may exist with respect to a person, a security vetting may be performed with respect to the following persons if requested by a head or directing body of an agency, specified in subsections 2 or 5 of § 27 of this Act:
1) a person who is about to be employed in a place of employment or a post which requires access to state secrets classified as 'restricted' upon discharging its functions, or who is already holding such a post;
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]
2) who is considered to be given access to state secrets classified as 'restricted' or who has the right of access, granted under the procedure specified in subsection 5 of § 27 of this Act.

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

(6) A security vetting may only be performed in case a person has given the consent for that purpose specified in clause 3 of subsection 10 of §27 of this Act unless otherwise provided in this Act. At the request of the agency which performs security vetting, the person specified in subsection 4 of this section must submit the questionnaire specified in clause 2 of subsection 1 of § 31 of this Act.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

§ 48. Security vetting agencies

(1) A security vetting shall be performed by the Internal Security Service, except in the cases specified in subsection 3 of this section.
[RT I 2008, 35, 213 – entry into force 01.01.2009]

(2) [Repealed –RT I 2008, 35, 213 – entry into force 01.01.2009]

(3) The Foreign Intelligence Service performs security vetting on the following persons:
1) a person applying for service or work at the Foreign Intelligence Service and the person serving or working there, with the exception of the Director General and their deputy and another official or employee of the Foreign Intelligence Service appointed by the Director General;
2) an active serviceman, official or employee appointed by the Commander of the Defence Forces, or a commander authorised thereby, whom the Foreign Intelligence Service wants to involve or has involved on the basis of § 41 of the Estonian Defence Forces Organisation Act;
3) the Director General of the Internal Security Service and their deputy and another official or employee of the Internal Security Service appointed by the Director General;
4) the Secretary General and the Deputy Secretary General of the Ministry of the Interior and an official directing and coordinating the work of the Internal Security Service in the Ministry of the Interior;
5) prosecutor.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

§ 49. Performance of security vetting

(1) The performance of security vetting and processing of personal data, including upon application of restrictions on the rights of the data subject, shall be based on the provisions of the Security Authorities Act, taking into account the specifications provided for in this Act.
[RT I, 13.03.2019, 2 – entry into force 15.03.2019]

(1^1) The processing of a special category of personal data shall be permitted upon verification of the circumstances specified in subsections 1 and 2 of § 32 of this Act.
[RT I, 13.03.2019, 2 – entry into force 15.03.2019]

(2) A committee, consisting of at least three members, is formed by an agency performing security vetting for the purpose of reviewing the information collected in the course of a security vetting.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(3) The committee, specified in subsection 2 of this section, shall make proposals to a person or a body that is competent to grant the right of access, a Personnel Security Clearance or Facility Security Clearance or extend the term thereof, adopt decisions concerning the revocation of the right of access or a Personnel Security Clearance or a Facility Security Clearance, adopt decisions concerning the issue of the right of access, a Personnel Security Clearance or a Facility Security Clearance, or adopt decisions concerning the extension of the term thereof on the basis of information collected as a result of a security vetting.

(4) For the purposes of a security vetting, the agency performing a security vetting shall conduct an interview, where necessary, with a person subject to a security vetting or, in the case of a legal person, with his or her legitimate representative (hereinafter referred to as 'applicant'). The agency performing the security vetting shall record the interview.
[RT I, 06.05.2020, 1 – entry into force 07.05.2020, applied retroactively from 1 March 2020]

(5) A person interviewed is questioned regarding the circumstances specified in § 32 and subsections 2 and 3 of § 42 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 a security vetting shall finish the performance of a security vetting immediately at the request of the person being vetted, the head of an agency specified in subsections 2 and 5 of § 27 of this Act, and a sponsor of a Personnel Security Clearance or a Facility Security Clearance. If this is the case, the person shall be refused the granting of the right of access or the granting of a Facility Security Clearance or extension of the term thereof or shall be deprived of the right of access to state secrets classified as 'restricted' or the granted Personnel Security Clearance or Facility Security Clearance shall 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 or her ability to interpret his or her behaviour or to control it incurs upon the conduct of a security vetting, an agency performing a 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 shall be refused the granting of the right of access or of a Facility Security Clearance or extension of the term thereof or shall be deprived of the right of access to state secrets classified as 'restricted' or the granted Personnel Security Clearance or Facility Security Clearance shall be revoked.

(8) The procedure for psychiatric examination to be performed during a security vetting and the form of conclusion shall be established by a regulation of the minister in charge of the policy sector.

Chapter 3
CLASSIFIED INFORMATION OF FOREIGN STATES

§ 50. General provisions

(1) Unless provided otherwise by an international agreement, the provisions applicable to the appropriate level of classification of state secrets, provided in Chapter 1, Chapter 2 Subchapter 3 and Chapter 4 of this Act are also applicable to the classified information of foreign states, considering the specifications detailed in this chapter.

(2) If the conformity of the classification level of the 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 based on the conformity of protective measures.

(3) International agreements shall serve as the basis for determining the term of classification of the 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, on wrong legal grounds or for a 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 or 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, on wrong legal grounds or for a 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) The processing system of classified information of foreign states must comply with the requirements set by the publisher of the classified foreign information. Compliance with the requirements is assessed under the conditions and procedure provided in § 46 of this Act.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(7) Regulations, adopted by the Government of the Republic under subsection 4 of § 20, subsection 13 of § 27, subsection 5 of § 31, subsection 3 of § 36, subsection 1 of § 39, subsection 6 of § 41, subsection 4 of § 42 and subsection 4 of § 46 of this Act, may establish specifications 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 imposed with regulations, adopted by the minister in charge of the policy sector under subsection 2 of § 39 of this Act.

§ 51. Access to classified information of foreign states

(1) Unless provided otherwise by an international agreement, the provisions provided in Chapter 2 Subchapter 3 Division 2 and 4 of this Act are also applicable to giving access to the classified information of foreign states, considering the specifications detailed in this Chapter.

(2) If the grounds for refusing the right of access, provided for in an international agreement, are stricter than the grounds stipulated in subsections 1 and 2 of § 32 or subsection 2–3 of § 42 of this Act, the existence of circumstances arising from an international agreement is also checked when a security vetting is performed and the existence of the appropriate circumstance shall serve as the grounds for refusing the granting of the right of access to classified information of foreign states. If the originator of classified information of foreign states prohibits granting of the right of access to a person, such person is not granted the right of access to respective classified information of foreign states.

(3) If an international agreement requires the performance of a security vetting for granting the right of access to classified information of foreign states, such security vetting shall be performed with respect to persons holding the right of access by virtue of office, except the President of the Republic.

(4) If the issue of a Personnel Security Clearance Certificate is specified in an international agreement as a pre-requisite for granting the right of 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') is issued to give access to classified information of foreign states. The National Security Authority shall issue the Personnel Security Clearance Certificate.

(4^1) The person specified in subsection 1 of § 30^1 of this Act, to whom it is desired to grant access to classified foreign information in addition to the right of access to a state secret, must submit a signed consent through the Defence Forces to the agency which performs security vetting, for the performance of the security vetting on the person, and the questionnaire specified in clause 2 of subsection 1 of § 31, in case it is prescribed in a treaty for obtaining the right of access to classified foreign information of the respective level.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(5) The National Security Authority shall immediately notify an agency performing a security vetting with respect to a person of the issue of a Personnel Security Clearance Certificate for access to classified information of foreign states to a natural or legal person, revocation or identification of invalidity of such certificate.

(6) Specific rules for the issue, refusal to issue, extension of the term and expiry of the term of validity of the right of access is established by a regulation of the Government of the Republic adopted under the Procedure of Protection of State Secrets and Classified Information of Foreign States.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

§ 52. Competence of National Security Authority for organisation of protection of classified information of foreign states

(1) The National Security Authority has the following functions under this Act, the legislation issued on the basis thereof and with international agreements:
1) organisation of the receipt of classified information of foreign states from the originator of the information, processing of and organising access to such information, registration of classified information of foreign states and the processing units who hold the information;
2) supervision over compliance with the requirements for the organisation of the protection of classified information of foreign states and for the processing of media by the processing unit, and the compliance with the requirements for the access of natural persons to the classified information of foreign states, including in foreign missions of the state and in the units of the Defence Forces located outside the territory of the Republic of Estonia;
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

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 Certificate 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, the 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 Cooperation Act, professional assistance from security authorities and the Defence Forces within the limits of their competence;
[RT I, 18.02.2014, 1 – entry into force 01.08.2014]
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) The National Security Authority does not organize or verify the following exchange of classified information of foreign states and the domestic transfer of classified information of foreign states, obtained in the process:
1) the exchange of classified information of foreign states, necessary for the performance of the tasks of a security agency, with an agency of a foreign state, international organization or an agency established under an international agreement, unless otherwise provided by an international agreement;
2) the exchange of classified information of foreign states, concerning the intelligence and counterintelligence of the structural unit of the Defence Forces dealing with military intelligence, with an agency performing intelligence or counter-intelligence tasks of a foreign state, unless otherwise provided by an international agreement;
3) the exchange of classified information of foreign states, concerning the witness protection by the Police and Border Guard Board, with an agency of a foreign state, international organization or an agency established under an international agreement, unless otherwise provided by an international agreement;
4) the exchange of classified information of foreign states at a level classified as “restricted”, corresponding to the characteristics specified in clauses 1–3 of § 8 of this Act, by a surveillance agency or prosecutor's office with an agency of a foreign state, international organization or an agency established under an international agreement, unless otherwise provided by an international agreement.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(4) Upon failure to comply with the precept, specified in clauses 3 and 4 of subsection 2 of this section, the National Security Authority has a right to apply substitutional performance and non-compliance levy in the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act and impose a non-compliance levy with a maximum value of 3,200 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

(5) Upon the termination of activities of an agency, institution, or a legal person in possession of classified information of a foreign state, or on demand of the National Security Authority, the media containing classified information shall be immediately transferred to the National Security Authority.

(6) The officials of the Estonian National Security Authority are entitled to carry a weapon during the performance of the duties provided for in this Act and use the weapon pursuant to the procedure provided for in this Act and the Weapons Act.
[RT I, 04.11.2016, 1 – entry into force 01.01.2017]

(7) [Repealed – RT I, 04.11.2016, 1 – entry into force 01.01.2017]

Chapter 4

LIABILITY

§ 53. Violation of requirements to protection of state secrets

(1) Violation of requirements for protection of state secrets by a person holding the right of access to state secrets in case it is accompanied by a risk 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 the incorrect legal grounds, at an incorrect level or for an incorrect term of classification, 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 3, 4 and 6 of subsection 1 of § 19, subsection 4 of § 32, subsection 6 of § 42 or § 45 of this Act are punishable for violation of notification obligation by a fine of up to 200 fine units or an arrest.
[RT I, 07.03.2023, 2 – entry into force 01.05.2023]

(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 penalty fine of up to 300 fine units or detention.

(3) Conduct specified in subsections 1–2 of this section if committed by a legal person shall be punishable by a penalty fine of up to 32,000 euro.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 54. Disclosure of state secrets due to negligence and loss of classified medium

(1) Disclosure, unlawful communication or allowing unlawful access to state secrets by a person, required to maintain the confidentiality of state secret if the conduct was due to negligence and also the loss of classified medium shall be punishable by a penalty fine of up to 300 fine units or an arrest.

(2) The same act if committed by a legal person shall be punishable by a penalty fine of up to 32,000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 55. Liability for violation of this Act

(1) 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.

(2) In case a person is deprived of the right of access to a state secret and classified information of a foreign state or the right for processing state secrets and classified information of a foreign state outside the immovable or movable held by a state authority, the Estonian Defence League or Eesti Pank for commitment of a misdemeanour under the State Secrets and Classified Information of Foreign States Act, such a person must apply again for the respective right for a Personnel Security Clearance or a Facility Security Clearance to obtain the right of access or the right to process.
[RT I, 27.01.2023, 1 – entry into force 01.04.2023]

(3) Provisions of the General Part of the Penal Code and the Code of Misdemeanour Procedure shall be applicable to the misdemeanour specified in this chapter.

(4) Extrajudicial proceedings in a misdemeanour specified in this chapter shall be conducted by the Internal Security Service.

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) The medium that is kept in an archive of a possessor of classified information shall be reviewed by the possessor of the information for the processing of classified media, as necessary, except the proceedings related to storage requirements and the inspection provided for in subsection 7 of § 20 of this Act.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(3) All the media, specified in subsection 2 of this section, must be reviewed, regardless of their processing needs by 1 January 2012 at the latest. The media shall be marked with the classification of state secret of the highest level, contained in the set of records.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

(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 or for different term for the purposes of this Act, the classification marking of a medium, the marking concerning the grounds of classification or term of classification shall be respectively changed.

(5) Section 15 or subsection 4 of § 50 of this Act shall apply as the grounds for considering declassification of information and changing the level, legal grounds or term of classification. Thereby there is no need to notify other agencies or constitutional institutions in advance of the intention of declassification or changing the level or term of classification and there is no need to hear their objections before such actions are conducted.
[RT I, 08.11.2010, 3 – entry into force 18.11.2010]

§ 57. Validity of right of access granted prior and performance of security vetting

(1) The Personnel Security Clearances, Personnel Security Clearance Certificates, temporary permits of use of processing systems and certificates of conformity, issued before the enforcement of this Act, shall remain valid until the expiry specified in such documents.

(2) An open-ended right of access, granted under subsection 3 of § 23 of the State Secrets Act 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 of access prior to this time.

(3) With respect to a person who has been granted a Personnel Security Clearance, a Personnel Security Clearance Certificate or who is holding the right of access on the basis of subsection 2 or 3 of § 23 of the State Secrets Act before the entry into force of this Act a security vetting may be performed under the conditions provided for in the State Secrets Act and pursuant to the procedure provided for in this Act until the expiry of such right of access or granting of the right of access under this Act.

§ 58. Access to state secrets after establishment of list of posts

(1) A person who is employed in a place of employment or a post where, after establishment of the list of posts specified in subsection 5 of § 20 of this Act, they are required to have the right of access to state secrets classified as "restricted" as a prerequisite for the performance of the tasks but who does not hold a valid Personnel Security Clearance, submits the documents specified in clauses 2 and 3 of subsection 10 of § 27 of this Act to the agency which performs a security vetting at the latest within one month after the entry into force of the list of posts specified above.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

(2) A person who is employed in a place of employment or a post where, after establishment of the list of posts specified in subsection 5 of §20 of this Act, they are required to have the right of access to state secrets classified as "confidential" or higher as a prerequisite for the performance of the tasks but who does not hold a valid Personnel Security Clearance that grants the right of access to state secrets of the respective level, submits an application for a Personnel Security Clearance for performing a security vetting with respect to that person to the agency which performs the security vetting at the latest within one month after the entry into force of the list of posts specified above.
[RT I, 07.03.2023, 7 – entry into force 01.04.2023]

§ 59.–§ 80.[Omitted from this text]

§ 81. Amendment of Riigikogu Internal Rules Act

[Omitted – RT I 2007, 44, 316 – entry into force14.07.2007]

§ 82.–§ 93.[Omitted from this text]

§ 94. Entry into force of the Act.

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