Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:

10 April 1997 [shall come into force on 6 May 1997];

4 December 1997 [shall come into force on 26 December 1997];

28 May 1998 [shall come into force on 30 June 1998];

18 March 1999 [shall come into force on 8 April 1999];

15 June 2000 [shall come into force on 14 July 2000];

13 December 2001 [shall come into force on 4 January 2002];

31 October 2002 [shall come into force on 4 December 2002];

18 December 2003 [shall come into force on 21 January 2004];

26 February 2004 [shall come into force on 31 March 2004];

27 May 2004 [shall come into force on 30 June 2004];

17 March 2005 [shall come into force on 15 April 2005];

11 May 2006 [shall come into force on 13 June 2006];

1 February 2007 [shall come into force on 28 February 2007];

29 March 2007 [shall come into force on 11 April 2007];

22 May 2008 [shall come into force on 18 June 2008];

10 December 2009 [shall come into force on 13 Jaunary 2010];

17 January 2013 [shall come into force on 19 February 2013];

15 May 2014 [shall come into force on 14 June 2014];

10 February 2017 [shall come into force on 10 February 2017];

1 February 2018 [shall come into force on 1 July 2018];

14 March 2019 [shall come into force on 20 March 2019];

13 June 2019 [shall come into force on 29 June 2019];

10 December 2020 [shall come into force on 1 January 2021];

20 April 2023 [shall come into force on 1 May 2023];

21 March 2024 [shall come into force on 6 April 2024].

If a whole or part of a section has been amended, the date of the amending law appears in square brackets at the end of the section. If a whole section, paragraph or clause has been deleted, the date of the deletion appears in square brackets beside the deleted section, paragraph or clause.

The *Saeima*1 has adopted and

the President has proclaimed the following law:

**On Official Secret**

**Section 1. Purpose of this Law**

(1) The purpose of the Law is to formulate the concept of an official secret, to prescribe the procedures for the storage and use of official secret and the protection thereof.

(2) The provisions of this Law shall not apply to information which has not been recognised as an official secret, but in respect of which special procedures for use and the prohibition of dissemination are prescribed by other laws or Cabinet regulations.

**Section 2. Concept of Official Secret**

(1) An official secret shall be such military, political, economic, scientific, technical or other type of information the loss or illegal disclosure of which may cause harm to the national security and economic or political interests of the State.

(2) Official secret subjects shall be State authorities, the officials and employees thereof, as well as other persons who, in connection with the performance of official (service) or work duties, create, obtain, keep or use official secret objects.

(3) An official secret object shall be information (data, aggregate of data) in any technically possible form of the recording thereof which, in accordance with this Law has been recognised or may be recognised as an official secret, as well as a material object, thing, substance or electromagnetic field which contains, keeps, accumulates or reflects information which has been recognised as an official secret in accordance with the procedures provided for by law.

(4) The status of an official secret shall be fully applicable to the classified information of the North Atlantic Treaty Organisation, the European Union, foreign and international organisations and their bodies, and protection of such information shall be ensured according to its classification level, unless provided otherwise in other laws and regulations.

[*18 December 2003; 17 March 2005; 20 April 2023*]

**Section 3. Classification Levels of an Official Secret**

(1) Information which is an official secret shall be classified according to the significance thereof as top secret, secret and confidential information, and information for official use.

(2) Information shall be recognised as top secret if it refers to the military, political, economic, scientific, technical, intelligence (counterintelligence), and operational activities of the State and the loss or illegal disclosure of it may cause:

1) military aggression against the Republic of Latvia or its allies or threats of such aggression, and real danger to national sovereignty;

2) severance of diplomatic relations or exclusion of the Republic of Latvia from international or intergovernmental organisations;

3) destabilisation of domestic political situation which leads to mass disorders, rioting, terrorist acts, sabotage, subversion or causes a necessity to announce a state of emergency or emergency readiness of the civil defence system;

4) disclosure of national defence plans or complicated encryption and intelligence communication systems;

5) disclosure of important plans in an investigatory process;

6) disclosure of nationally significant scientific or technological discoveries.

(3) Information shall be recognised as secret if it refers to the military, political, economic, scientific, technical, intelligence (counterintelligence), and operational activities of the State and the loss or illegal disclosure of it may cause:

1) aggravation of international relations;

2) aggravation of intergovernmental relations as a result of which economic relations are severed or economic sanctions are imposed on the Republic of Latvia;

3) disclosure of significant military plans or intelligence (counterintelligence) measures;

4) disclosure of the content of work organisation, methods, tactics or investigatory records of bodies performing operational activities;

5) disclosure of the plan of significant operational activities measures or identities of persons involved in these activities;

6) disclosure of scientific or technological discoveries related to national defence and security or the development of a specific economic sector.

(4) Information shall be recognised as confidential if it refers to military, political, economic, scientific, technical, intelligence (counterintelligence), and operational activities and the loss or illegal disclosure of it may jeopardise State interests, causing harm to a specific State authority.

(5) [18 December 2003]

(6) Information shall be recognised as information for official use if it is designated by the head of an institution and related to the performance of the functions of the institution, intended to ensure operating activities of the institution, and the loss or illegal disclosure of which may jeopardise State interests, including national security, security of the field, or security of the institution.

[*31 October 2002; 18 December 2003; 20 April 2023*]

**Section 4. Recognition of Information as an Official Secret**

(1) A list of information and other objects to be recognised as a confidential, secret, and top secret official secret, the amount and content thereof shall be determined by the Cabinet in compliance with the principles and information classification provisions set out in this Law, and also the proposals of the National Security Council and the Constitution Protection Bureau. The list of information and other objects to be recognised as an official secret approved by the Cabinet, as well as subsequent amendments thereto shall be considered to be public documents.

(2) The following information may be recognised as an official secret:

1) information on the military potential, defence strategy and tactics, defence and mobilisation plans of the State;

2) information on the armament, communications and information systems, material and technical facilities of national security and defence institutions and the acquisition thereof;

3) information on the layout of structures, installations, facilities, and other sites of significance for national security and defence, defence and evacuation plans;

4) information on the types and amount of products manufactured for national security and defence purposes, as well as the potential of the facilities;

5) information on ciphers (codes), encryption systems, and equipment;

6) information on the organisation, content, tactics, and methods of operational activities, intelligence and counterintelligence, as well as on the persons involved in the performance of operational activities and persons involved in the special procedural protection;

7) information on the deployment of the structures and individual units of State security institutions;

8) information on the action and activity plans of the units of the Ministry of the Interior, national security and defence institutions in case of a state of emergency, mass disorders or on special operations in the fight against organised crime;

9) information on the amount, location and holders (keepers) of State material reserves;

10) information on the storage and transportation of national currency and precious metal reserves;

11) information on the organisation of security guards and security measures for significant State officials and the technical means applied;

12) information on scientific research activities, discoveries, use of inventions if they are performed with State support;

13) information on the separate directions of the State foreign policy activities and external economic relations of strategic significance;

14) information on the means and techniques for the protection of an official secret;

15) information which Latvia has received from foreign countries or has created in accordance with an entered into international agreement.

(3) If information and objects recognised as an official secret need to be used for ensuring the development and operation of publicly accessible information, objects and projects, they shall be prepared for public use in the form of general statistical data or in any other indirect form and shall be issued only in the amount permitted and used only for the purposes for which the issue thereof was permitted.

(4) Unauthorised extension of the status and amount of information or other secret information and objects included in the list of objects to be recognised as an official secret and the attribution thereof to information and objects which have been and are publicly usable and accessible is prohibited.

(5) A person has the right to become acquainted with the list of information for official use only designated by the head of the institution that includes types of information, topics, individual documents, and types thereof.

[*18 March 1999; 31 October 2002; 20 April 2023*]

**Section 5. Information which May not be an Official Secret**

It is prohibited to grant the status of an official secret and to restrict access to the following information:

1) information on natural disasters, natural or other calamities, and the consequences thereof;

2) information on the environmental, health protection, educational, and cultural state, as well as the demographic situation;

3) information on violations of human rights;

4) information on the crime rate and the statistics thereof, corruption cases, irregular conduct of officials;

5) information on the economic situation of the State, implementation of the budget, living standards of the population, as well as the wage rates, privileges, advantages, and guarantees specified for officials and employees of State and local government authorities;

6) information on the state of health of the heads of State.

**Section 6. State Ownership Rights to Official Secret Objects**

(1) The State has exclusive ownership rights to official secret objects and they shall be under special State protection.

(2) An official secret object which is owned by a legal or natural person may be alienated for the purposes of official secret protection without the consent of the owner, paying to him or her an appropriate compensation. The amount of the compensation shall be determined by mutual agreement of the parties, but if no agreement has been reached, a court shall determine it. In claims regarding the determination of the amount of compensation, the parties shall be exempt from the payment of court costs.

(3) An official secret object may be in the possession or use of a person in such cases and in accordance with such procedures as prescribed by law or Cabinet regulations.

**Section 7. Protection of an Official Secret**

(1) Protection of an official secret shall be a purposeful activity of a legal, technical and organisational nature by competent State authorities and the officials thereof in order to ensure the preservation of an official secret and to prevent the illegal dissemination (use) thereof.

(2) Protection of an official secret shall be organised by the Cabinet. For this purpose, the Cabinet shall, taking into account the principles set out by law, issue regulations regarding the procedures for the classification, declassification, signing, receipt, registration, storage, issuing, use, sending, conversion into electronic form, and destruction (classified registry) of official secret objects, the documentation of this process, the use of special designations, ciphers (codes), as well as take other measures of technical and organisational nature.

(3) The Constitution Protection Bureau, the Defence Intelligence and Security Service, and the State Security Service shall, in conformity with the competence of these institutions set out by law, manage, coordinate, control, and take measures for the protection of an official secret.

(4) The heads of the authorities or of the relevant units thereof within the competence thereof shall be responsible for compliance with the secrecy regime and ensuring protection of an official secret in State authorities. These officials shall be responsible for ensuring that the employees subordinate to them whose work (service) is related to an official secret are provided with conditions suitable for this work in accordance with Cabinet regulations. If an authority has at its disposal such material objects to which the status of an official secret or classified information of the North Atlantic Treaty Organisation, the European Union, or foreign classified information has been assigned and in circulation thereof the requirements of classified registry may not be applied, the head of the authority himself or herself shall determine the protection measures for these material objects by agreeing thereupon with the competent State security institution. At the request of the head of the relevant authority, employees of State security institutions may be assigned to ensure the secrecy regime.

(5) The provisions of Paragraph four of this Section shall also apply to other persons having official secret objects, classified information of foreign countries or international organisations and their bodies in their possession or use. A merchant that needs to use a confidential, secret, and top secret official secret, classified information of foreign countries or international organisations and their bodies in its work must receive a facility security clearance which shall be issued to it by the Constitution Protection Bureau after a security vetting performed by a State security institution. The procedures for the submission of an application for the receipt of a facility security clearance, the list of the documents to be submitted, periods, procedures for the issue, registration, use, change of level or cancellation of facility security clearance shall be governed by the Cabinet regulations. The director of the Constitution Protection Bureau shall specify the procedures for the performance of a security vetting. The decision of the director of the Constitution Protection Bureau to refuse to issue a facility security clearance or to cancel it may be contested and appealed by a merchant in accordance with the same procedures as the decision to refuse, cancel or lower the level of the personnel security clearance for access to an official secret. The decision of the director of the Constitution Protection Bureau to refuse to issue a facility security clearance or to cancel it in relation to the right to use the classified information of foreign countries, international organisations and their bodies shall be final and not subject to appeal. If the decision to refuse to issue a facility security clearance or to cancel it is taken, the Constitution Protection Bureau shall ensure informing and hearing of a merchant in accordance with the same procedures which are intended for a person who qualifies for the access to an official secret.

(51) When fulfilling a government order of the Republic of Latvia, a merchant registered in a foreign country may be permitted to use official secret objects, classified information (top secret, secret or confidential) of the North Atlantic Treaty Organisation, the European Union, if the competent authority of the relevant country has issued the merchant with a facility security clearance of appropriate level which has been recognized as being valid for use in the Republic of Latvia by the Constitution Protection Bureau, and if this has been provided for in the agreement for mutual protection of classified information entered into by the Republic of Latvia and the relevant country.

(6) The Constitution Protection Bureau shall, as the national security authority of the Republic of Latvia, itself perform and control exchange of classified information with foreign countries, international organisations and their bodies, as well as take measures for the protection of such information.

(7) All State and local government authorities, and also legal and natural persons may only process or store a confidential, secret, and top secret official secret in information systems that are registered with and accredited by the Constitution Protection Bureau, except for information systems which are only intended for the acquisition, processing, and storage of signals intelligence information and are registered with and accredited by the Defence Intelligence and Security Service in accordance with the procedures laid down by the Defence Intelligence and Security Service. The Constitution Protection Bureau shall also register and accredit information systems which are intended for processing or storing information for official use only if these information systems are connected to the public electronic communications network. The Constitution Protection Bureau shall lay down the procedures for the registration, security checks, and accreditation of information systems. The Defence Intelligence and Security Service shall inform the Constitution Protection Bureau about the information systems registered with the Defence Intelligence and Security Service and the accreditation status thereof. The Constitution Protection Bureau shall, as the security accreditation authority, control the cryptographic system of the official secret and develop cryptographic keys.

(71) An electronic document containing the official secret shall be deemed to be signed by hand and it shall have legal effect if it has been signed with an electronic signature within the meaning of Article 3(10) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. For electronic signing of the document containing the official secret, the national security authority shall approve in accredited information systems an appropriate electronic signature or establish and maintain a common electronic signature infrastructure.

(72) The authority has the right to convert the documents containing the official secret which are prepared in paper form and registered into electronic form for storage in an electronic data medium and to destroy the paper documents. The document converted into electronic form shall have the same legal effect as the original of the document.

(8) Procedures for the receipt, delivery, and use of the classified information of foreign countries, international organisations and their bodies shall be governed by Cabinet regulations. Such information shall be protected as an official secret and nobody is entitled to downgrade the classification level thereof without the consent of the dispatching country or organisation.

(9) The Defence Intelligence and Security Service as the national institution of signals intelligence shall carry out and control signals intelligence information exchange with foreign national authorities, international organisations and their bodies, as well as implement measures for the protection of such information.

[*28 May 1998; 13 December 2001; 31 October 2002; 18 December 2003; 27 May 2004; 17 March 2005; 11 May 2006; 1 February 2007; 29 March 2007; 10 December 2009; 15 May 2014; 1 February 2018; 14 March 2019; 20 April 2023; 21 March 2024*]

**Section 8. Periods for the Retention of Secrecy of an Official Secret**

(1) For information for official use only, secrecy shall be specified for three years, for confidential information – for five years, for secret information – for ten years, for top secret information – for twenty years, but for data on persons involved in the performance of operational activities and persons who are involved in special procedural protection – for seventy-five years.

(2) Before the end of the secrecy term of the relevant information, the authority which classified it shall decide on the determination of a new secrecy term or declassification of the information.

(3) If the secrecy term specified by the law has expired or the relevant information as an official secret has lost its significance before the specified term, the secrecy for this information shall be cancelled and it shall become available to the public.

[*18 March 1999; 31 October 2002; 18 December 2003; 20 April 2023*]

**Section 9. Accessibility of an Official Secret**

(1) Access to an official secret shall only be permitted to a person who, in accordance with the official (service) duties or a specific work (service) task, is required to perform work related to the use or protection of an official secret and who:

1) has received the personnel security clearance in accordance with this Law if he or she requires access to confidential, secret, or top secret information;

2) has signed and submitted a non-disclosure agreement to the head of the institution that he or she undertakes to keep and not illegally disclose information if he or she requires access to information for official use.

(11) Security vetting of a person for access to confidential, secret, and top secret information shall be carried out before commencing work with the official secret.

(2) The personnel security clearance for access to a confidential, secret, and top secret official secret (hereinafter – the personnel security clearance) may be issued to a citizen of Latvia who is not younger than 18 years of age, in relation to whom the trusteeship has not been established, who has signed a non-disclosure agreement that he or she undertakes to keep and not illegally disclose the official secret and has agreed that competent State security institutions shall take the necessary measures for the security vetting of the person and protection of the official secret.

(3) Access to confidential, secret and top secret official secret objects shall be denied to a person:

1) who has submitted a renunciation of the Latvian citizenship;

2) whose capacity to act is limited in accordance with the procedures specified by law;

3) who:

a) has been convicted for an intentional criminal offence or disclosure of an official secret through negligence – regardless of whether or not the criminal record has been extinguished or set aside;

b) has been convicted of an intentional criminal offence or disclosure of an official secret through negligence by releasing him or her from the punishment;

4) who is or has been a staff employee or a non-staff employee of the security service, intelligence or counterintelligence service of the USSR, Latvian SSR or a foreign country other than the member states of the European Union or the North Atlantic Treaty Organisation, or an agent, resident or safe-house keeper thereof;

5) who, after 13 January 1991, has worked in the CPSU (LCP), the Working Peopleʼs International Front of the Latvian SSR, the United Council of Labour Collectives, the Organisation of War and Labour Veterans or the All-Latvia Salvation of Society Committee;

6) in respect of whom, during the security vetting, facts have been established that provide a basis for:

a) doubting his or her reliability and ability to keep an official secret;

b) deeming that the issuing of the personnel security clearance does not correspond to the national security interests;

7) who has been found having mental and behavioural disorders, including as a result of the use of alcohol, narcotic, psychotropic or toxic substances that provide a basis for doubting his or her ability to meet the conditions for the protection of an official secret;

8) [18 December 2003].

(31) [18 December 2003]

(32) The Cabinet shall determine the medical contraindications referred to in Paragraph three, Clause 7 of this Section for the issue of the personnel security clearance and the procedures by which a person is sent to the health examination, and also medical treatment institutions in which a commission for the health examination is established, the work organisation of such commission, the procedures for the performance of and payment for the health examination.

(4) On the basis of a proposal by the authority which has initiated a security vetting or upon his or her own initiative, the head of the State security institution may, subsequent to the performance of the security vetting, grant access to a confidential, secret, and top secret official secret to individual persons for which it is restricted by the provisions of Paragraph three, Clause 3 of this Section if an especially serious crime has not been committed – regardless of whether the conviction has been extinguished or set aside.

(5) [1 February 2018]

(51) Upon recommendation of the commander of the National Armed Forces and after performance of a security vetting, the director of the Constitution Protection Bureau may grant soldiers of the National Armed Forces who after 13 January 1991 have been members of the CPSU (LCP) access to a confidential, secret, and top secret official secret, if they have proved their loyalty towards the State of Latvia.

(6) If the personnel security clearance to a person is not issued, it is a sufficient ground to refuse his or her employment in a position which is related to the use or protection of an official secret.

(7) Procedures by which an official secret shall be transferred to representatives of foreign countries within the framework of co-operation between the Republic of Latvia and foreign countries shall be determined by the Cabinet.

(8) During emergency situations, war, or state of emergency, the head of an authority may allow a person who has been issued the personnel security clearance to access an official secret of a higher classification level or classified information of foreign countries, international organisations and their bodies. During emergency situations, war, or state of emergency, the head of an authority may allow a person who has not been issued the personnel security clearance to access confidential, secret, and top secret official secret or classified information of foreign countries, international organisations and their bodies. In the abovementioned cases, the head of the authority shall inform the competent State security institution. The conditions, terms, and procedures by which the head of the authority grants the respective clearances and informs the competent State security institution shall be determined by the Cabinet.

[*15 June 2000; 31 October 2002; 18 December 2003; 26 February 2004; 27 May 2004; 17 March 2005; 15 May 2014; 1 February 2018; 13 June 2019; 20 April 2023* / *Paragraph eight shall come into force form 1 January 2024. See Paragraph 13 of Transitional Provisions*]

**Section 9.1 Suitability of a Merchant for Obtaining a Facility Security Clearance**

(1) Facility security clearance confirms the readiness and ability of a merchant to carry out the work with a confidential, secret, and top secret official secret object and ensure protection thereof.

(2) Facility security clearance may be issued to a merchant:

1) which is registered with the Enterprise Register of the Republic of Latvia;

2) which has been established at least two years ago and is carrying out its commercial activities;

3) which has submitted to a State security institution all the documents necessary for security vetting laid down in laws and regulations within the specified term and has indicated the justification which confirms the necessity to obtain a facility security clearance;

4) which has agreed that a State security institution shall perform the security vetting of a merchant and persons related thereto.

(3) Issuing of a facility security clearance shall be refused or facility security clearance shall be cancelled if:

1) during the security vetting such facts were established in respect of a merchant that provide a basis for doubting its reliability and ability to keep the official secret;

2) a merchant has refused to comply with or has violated instructions of a State security institution in relation to the protection of an official secret or has provided false information;

3) a coercive measure laid down in the Criminal Law has been imposed on a merchant within the last five years.

(4) Issuing of a facility security clearance may be refused or facility security clearance may be cancelled if:

1) violation of the provisions for the protection of official secret objects has been established in the activities of a merchant;

2) a merchant has a tax debt.

[*1 February 2018; 20 April 2023*]

**Section 10. Examination of the Compliance of Persons and Premises with Security Requirements**

(1) If a question regarding the issue of personnel security clearances to specific persons is being decided, State security institutions shall, within the competence thereof, perform a security vetting of such persons and provide an opinion on the possibility to issue the personnel security clearance.

(2) The term of security vetting of a person shall be three months. If due to objective reasons the term of three months cannot be complied with, the head of a State security institution may extend it for another three months by notifying a person thereof. Organisation, methods, tactics, resources and other issues of the security vetting process of the person to be complied with during the security vetting process of the person shall be determined by the Council of State Security Institutions after agreement thereupon with the Prosecutor General.

(3) In the *Saeima*, the Chancery of the President, the State Chancellery, the State Audit Office, Latvijas Banka, the Ministry of Foreign Affairs, the Office of the Prosecutor and the Corruption Prevention and Combating Bureau, the security vetting of the compliance of persons and premises with security requirements shall be performed by the Constitution Protection Bureau. The Constitution Protection Bureau shall also perform, at all authorities, a security vetting of the heads of units responsible for ensuring the secrecy regime.

(31) [29 March 2007]

(4) At the Ministry of Defence, authorities subordinate thereto, the National Armed Forces, military sites, as well as institutions, organisations and merchant undertakings if their activities are related to an official secret in the area of military defence, security vetting of the compliance of persons and premises with security requirements shall be performed by the Defence Intelligence and Security Service. In other authorities, security vetting of the compliance of persons and premises with security requirements shall be performed by the State Security Service.

(5) If the information obtained during the security vetting which may be the basis for the person to be denied access to a confidential, secret, and top secret official secret must be evaluated, a State security institution shall ensure hearing of the person who qualifies for access to a confidential, secret, and top secret official secret or to whom the personnel security clearance for the work with an official secret has been issued.

(6) In accordance with the Law on Notification, a State security institution shall notify the time when a person must arrive for hearing to the person to be vetted and the authority which has initiated the security vetting. During the hearing, a State security institution shall acquaint a person with a summary of the vetting file where the reasons due to which access to an official secret may be denied for the person are indicated. After the person to be vetted has been acquainted with the summary of the vetting file, the State security institution shall hear explanation of the person to be vetted on the facts referred to in the summary of the vetting file. The State security institution shall append the explanation of the person to the case file.

(7) A person has the obligation to arrive at a State security institution at the time indicated. The State security institution may postpone the hearing of a person to another time due to illness of a person or other justifying reasons. If a person fails to arrive to the hearing without any justifying reason at the time indicated by the State security institution, it shall be regarded that he or she has refused to exercise his or her right to be heard in the relevant stage of the security vetting process.

(8) A State security institution is entitled to complete security vetting and take a decision without hearing a person if:

1) the person has failed to arrive to the hearing without any justifying reason at the time indicated by the State security institution or has not informed the State security institution of the necessity to change the hearing time due to a justifying reason;

2) the person, due to a justifying reason, may not repeatedly arrive to the postponed hearing at the State security institution, but the information obtained during the security vetting is sufficient for the State security institution to take a decision;

3) it is necessary to immediately cancel the personnel security clearance issued to the person in the interests of national security.

(9) If the decision is taken to deny access to a confidential, secret, and top secret official secret for a person, a State security institution shall, after taking the decision, inform such person of the reasons of such decision in writing without disclosing the information which may:

1) be harmful to the rights or legal interests of another person;

2) disclose covert assistants or persons which have confidentially provided assistance;

3) disclose front organisations or other means of masking;

4) disclose work organisation, methodology or tactics of the State security institutions;

5) be harmful to the performance of the tasks of intelligence, counterintelligence, operational activities, or pre-trial criminal proceedings;

6) disclose means or techniques for the protection of an official secret;

7) be harmful to the co-operation with foreign special services, law enforcement institutions or organisations.

(10) Within the framework of a security vetting, a State security institution shall assess the conformity of a person to the requirements of this Law by examining the information provided by him or her and assessing the information which is publicly available on the person or can be obtained in conformity with the Law on State Security Institutions and Operational Activities Law.

(11) A State security institution shall inform the authority which has initiated a security vetting of the decision taken as a result of the security vetting.

(12) Security vetting of persons in relation to access to the classified information of foreign countries, international organisations and their bodies shall be performed and clearances shall be issued by national security authority of the Republic of Latvia. The procedures and period for the security vetting of persons shall be specified by the director of the Constitution Protection Bureau.

[*17 March 2005; 1 February 2007; 29 March 2007; 17 January 2013; 1 February 2018; 14 March 2019; 20 April 2023*]

**Section 11. Issue of Personnel Security Clearances**

(1) Personnel security clearances shall be issued for a specific term which shall not be longer than five years. Personnel security clearances shall be divided into three levels.

(2) Access to top secret information shall be permitted to a person with a first level personnel security clearance, to secret information – with a second level personnel security clearance, and to confidential information – with a third level personnel security clearance.

(3) A person having the personnel security clearance for access to information of a higher classification level shall also concurrently have access to information of a lower classification level.

(4) Procedures for the registration, issue, cancelation, and changing the level of personnel security clearances shall be regulated by Cabinet regulations.

(5) The decision to refuse to issue the personnel security clearance shall come into effect at the time of taking thereof, and a person may contest and appeal such decision in accordance with the procedures provided for in Section 16 of this Law.

(6) The decision of the director of the Constitution Protection Bureau on access to the classified information of foreign countries, international organisations and their bodies shall be final and may not be appealed.

(7) [20 April 2023]

[*31 October 2002; 18 December 2003; 17 March 2005; Constitutional Court Judgment of 10 February 2017; 1 February 2018; 20 April 2023*]

**Section 12. Right to Use an Official Secret**

(1) The right to use a confidential, secret, and top secret official secret for each specific person shall be restricted by the term of validity for which the personnel security clearance has been issued to him or her, as well as the cancellation of the personnel security clearance.

(2) The list of positions related to the use and protection of an official secret at each authority shall be determined by the head of the relevant authority.

(3) Access to a confidential, secret, and top secret official secret and the right to use it for the performance of official (service) duties, if there are not the restrictions specified in Section 9, Paragraph three of this Law, on the basis of the position held thereof, shall have the following:

1) the President;

2) the chairperson of the *Saeima*;

3) the Prime Minister;

4) members of the *Saeima*;

5) members of the Cabinet;

6) the President of the Supreme Court;

7) the Prosecutor General;

8) the Auditor General;

9) the supreme commander and commander of the National Armed Forces;

10) the commander of the National Guard;

11) the director of the Constitution Protection Bureau, the chief of the Defence Intelligence and Security Service, the chief of the State Security Service;

12) the Governor of Latvijas Banka;

13) the director of the Corruption Prevention and Combating Bureau;

14) [29 March 2007];

15) the Ombudsman;

16) the members of the National Electronic Mass Media Council;

17) the chairperson of the Central Election Commission;

18) the members of the Council of Latvijas Banka;

19) the members of the Public Electronic Mass Media Council and the members of the Board of the Public Electronic Mass Media;

20) the chairperson of a local government council and vice-chairperson.

(4) Parliamentary investigation commissions appointed by the *Saeima* shall have access to an official secret and the right to use it for the performance of the duties thereof.

(5) The person directing the proceedings (inquiry performer, prosecutor, judge) shall have access to an official secret and the right to use it within his or her competence in a pre-trial investigation and proceedings in a specific criminal matter which is related to an official secret. Persons taking part in the investigation process and court proceedings of such matter and having the right to acquaint themselves with all the materials of the matter shall be warned in writing of the obligation to keep an official secret and the liability provided for the illegal disclosure of an official secret. Such procedures shall also be applicable to persons taking part in court proceedings of a civil case, administrative case or administrative offence case, if it is related to the official secret.

(6) It is prohibited to illegally disclose an official secret or to use it for purposes other than the performance of the official (service) duties or specific work tasks.

[*4 December 1997; 28 May 1998; 13 December 2001; 31 October 2002; 27 May 2004; 17 March 2005; 1 February 2007; 29 March 2007; 22 May 2008; 15 May 2014; 1 February 2018; 14 March 2019; 13 June 2019; 10 December 2020; 20 April 2023; 21 March 2024*]

**Section 13. Cancelling, Lowering the Level of Personnel Security Clearances and Consequences of Denying Personnel Security Clearances**

(1) The personnel security clearance shall be cancelled if:

1) a person has been removed from a position (work) related to the use or protection of a confidential, secret, and top secret official secret;

2) a person has violated the procedures prescribed for work with a confidential, secret, and top secret official secret, the use or protection thereof;

3) the circumstances specified in Section 9, Paragraph three of this Law have been discovered;

4) it has become known that the person has knowingly provided false information on himself or herself.

(2) The circumstances referred to in Paragraph one, Clauses 2–4 of this Section may also serve as a basis for lowering the level of personnel security clearance.

(3) The decision to cancel the personnel security clearance or lower the level thereof shall come into effect at the time of taking thereof, and a person may contest and appeal such decision in accordance with the procedures provided for in Section 16 of this Law. If the decision to cancel the personnel security clearance or lower the level thereof is taken on the basis of the circumstances referred to in Paragraph one, Clauses 2, 3, or 4 of this Section, a State security institution shall ensure the informing and hearing of the person referred to in Section 10 of this Law.

(4) If the personnel security clearance of a person is refused or the personnel security clearance is cancelled on the basis of Paragraph one, Clause 2, 3, or 4 of this Section, it shall be a sufficient reason to believe that this person is not suitable for the position held (work to be performed) which is related to the use or protection of a confidential, secret, or top secret official secret. After taking the decision, such person shall be immediately transferred to the position which is not related to a confidential, secret, and top secret official secret, or, where it is not possible, immediately suspended from performing his or her official duties, retaining the monthly wage and social guarantees of the position. After taking the final decision, such person shall be immediately transferred to the position which is not related to a confidential, secret, and top secret official secret, or, where it is not possible, employment (service) relations shall be immediately terminated with him or her.

(41) After taking the decision to lower the level of the personnel security clearance, a person shall be immediately transferred to an appropriate position, or, where it is not possible, immediately suspended from performing his or her official duties, retaining the monthly wage and social guarantees of the position. After taking the final decision, such person shall be immediately transferred to an appropriate position, or, where it is not possible, employment (service) relations shall be immediately terminated with him or her.

(5) Termination of employment (service) relations with a person who, in relation to the performance of work (service) duties, had access to an official secret shall not release such person from the obligation to keep an official secret and the liability for illegal disclosure thereof.

[*18 December 2003; Constitutional Court Judgment of 10 February 2017; 1 February 2018; 20 April 2023*]

**Section 13.1 Repeated Assessment of the Person who has been Denied Access to an Official Secret**

(1) A person who has been denied access to a confidential, secret, or top secret official secret and who, in accordance with the official (service) duties or a specific work (service) task, is required to carry out work related to the use or protection of the confidential, secret, or top secret official secret has the right to repeatedly apply for obtaining the personnel security clearance in accordance with the procedures laid down in this Section.

(2) If the decision to refuse or cancel the personnel security clearance has been taken previously, the access to a confidential, secret, and top secret official secret may be assessed five years after:

1) regaining the citizenship of Latvia if Section 9, Paragraph three, Clause 1 of this Law has been applied;

2) renewal of capacity to act if Section 9, Paragraph three, Clause 2 of this Law has been applied;

3) coming into effect of the decision to refuse or cancel the personnel security clearance if Section 9, Paragraph three, Clauses 6 or 7 or Section 13, Paragraph one, Clauses 2 or 4 of this Law has been applied.

(3) If the decision to refuse or cancel the personnel security clearance has been taken previously on the basis of Section 9, Paragraph three, Clauses 3, 4, or 5 of this Law, a person shall henceforth be denied the receipt of the personnel security clearance, except when the basis for the establishment of the fact provided for in the abovementioned Clauses has ceased to exist.

(4) A State security institution shall commence the security vetting of a person for the issue of the personnel security clearance in accordance with Paragraphs two and three of this Section after proposal of the authority which has initiated the security vetting.

[*1 February 2018; 20 April 2023*]

**Section 14. Obligations of a Person in Respect of an Official Secret**

(1) A person who is entitled to carry out work which is related to an official secret or the protection thereof shall be personally liable for the fulfilment of the requirements for the protection of an official secret provided for in the law and Cabinet regulations and compliance with the specified secrecy regime and classified registry regulations.

(2) If the circumstances referred to in Section 9, Paragraph three of this Law have arisen which deny the person the access to a confidential, secret, and top secret official secret, the person has the obligation to notify the authority which issued the personnel security clearance thereof without delay.

(3) An official secret subject shall, without delay, notify the relevant State security institution of the cases of the loss of official secret objects and in co-operation with this institution shall carry out a search for the lost objects, as well as take the necessary measures to prevent or diminish harm which may arise as a result of disclosure of the official secret.

[*20 April 2023*]

**Section 15. Liability for Violation of Regulations for the Use or Protection of an Official Secret**

(1) A person who by his or her action or failure to act has violated the regulations for the use or protection of an official secret shall be held disciplinary or criminally liable in accordance with the procedures set out by law.

(2) Procedures for the internal investigation of such matters shall be determined by the Cabinet.

**Section 16. Procedures for Contesting and Appealing the Decision to Refuse, Cancel or Lower the Level of the Personnel Security Clearance**

(1) A person may contest the decision to refuse, to cancel or lower the level of the personnel security clearance to the Prosecutor General within 14 days of the day of its announcement.

(2) A person may appeal the decision of the Prosecutor General to the Regional Administrative Court within 14 days after the day of its announcement. Contesting and appeal of such decision shall not suspend the operation thereof. The operation of the decision shall not be suspended also upon request of the person.

(3) In the proceedings for the contesting and appeal of the decisions provided for in Paragraphs one and two of this Section, the norms of the Administrative Procedure Law shall be complied with, insofar as this Law does not determine other procedures.

[*1 February 2018*]

**Section 17. Examination of Applications in Court**

(1) The Regional Administrative Court shall examine the case which has been initiated on the basis of the application for the decision referred to in Section 16, Paragraph two of this Law within two months from the day of taking the decision to accept the application and to initiate a case.

(2) The court shall examine the case as the court of first instance. The case shall be examined collegially in the composition of three judges.

(3) The court shall verify whether the appealed decision is lawful. The court shall, when assessing the lawfulness of the decision, take into account not only the justification included in the decision, but also the information containing an official secret which was the basis for taking the appealed decision.

(4) The amount of the information to be disclosed to a person which contains an official or investigative secret shall be determined by a State security institution in compliance with Section 10, Paragraph nine of this Law. If disclosure of such information to a person is denied, the information containing an official or investigative secret shall be verified and evaluated only by the court. In such case the court shall indicate in the ruling that the information has been evaluated.

(5) The court ruling is not subject to appeal and shall enter into effect at the moment of its proclamation. The court ruling shall be sent to a State security institution for enforcement.

[*1 February 2018; 20 April 2023*]

**Section 18. Procedure for Contesting and Appealing the Refusal to Provide Information for Official Use Only**

A person may contest and appeal the refusal to provide information for official use only in accordance with the procedures laid down in the Administrative Procedure Law. When examining the case, the court shall also assess the grounds for information classification.

[*20 April 2023*]

**Transitional Provisions**

1. The Cabinet shall, by 15 December 1996, draft the legal acts necessary for the implementation of this Law.

2. Persons currently holding positions which are related to the use and protection of an official secret must, within three months from the coming into force of this Law, receive personnel security clearances for access to an official secret in conformity with the provisions of this Law, or they shall be transferred to a position which is not related to an official secret.

3. In respect of employees of the institutions of the Ministry of the Interior holding positions which are related to an official secret in the area of operational activities, if they have been appointed to these positions before the coming into force of this Law, the provisions of Section 9, Paragraph two, Clause 2 of the Law shall come into force one year after they have been given a possibility, within the term specified in the Citizenship Law, to acquire Latvian citizenship in accordance with the general naturalisation procedures.

[*10 April 1997*]

4. Authorities storing information to which the official secret classification level “ierobežotas lietošanas informācija” [restricted use information] has been assigned shall declassify this information by assigning to it the status “informācija dienesta vajadzībām” [information for official use only] in conformity with the Freedom of Information Law.

[*18 December 2003*]

5. When deciding on the cancellation of such personnel security clearance which has been issued until 30 June 2018 or lowering of the level, the wording of Section 9, Paragraph three, Clause 3 of this Law which was in force until 30 June 2018 shall be applied.

[*1 February 2018*]

6. If access to an official secret has been denied to a person before 1 July 2018, a repeated assessment of the person in accordance with the provisions of Section 13.1 of this Law may be initiated and security vetting may be commenced after 10 February 2022.

[*1 February 2018*]

7. The Constitution Protection Bureau shall, after 1 July 2018, complete the examination of the cases in its proceedings on the appealed decisions to refuse, cancel the personnel security clearance, to not extend the term or lower the level of the personnel security clearance. A person may appeal the decision of the director of the Constitution Protection Bureau to a Regional Administrative Court within 14 days after the day of its announcement.

[*1 February 2018*]

8. A person may appeal the decision taken by the Prosecutor General until 30 June 2018 in accordance with Section 7, Paragraph five or Section 11, Paragraph five of this Law to a Regional Administrative Court within 14 days after the day of its announcement.

[*1 February 2018*]

9. The court shall take a ruling in the cases which have been initiated in conformity with Section 17, Paragraph one of this Law until 31 December 2018 within a year from the day when the decision to accept the application and initiate the case was taken.

[*1 February 2018*]

10. The Cabinet shall issue the regulations provided for in Section 9, Paragraph 3.2 of this Law by 31 December 2018. Until issuing the abovementioned regulations, mental disorders, addiction to alcohol, narcotic, psychotropic, toxic substances or behavioural disorders which provide a basis for doubting a person’s ability to meet the conditions for the protection of an official secret shall be established in accordance with the same procedures which were applied until the day of coming into force of Section 9, Paragraph 3.2of this Law.

[*1 February 2018*]

11. If the application for issuing a facility security clearance is issued until 30 June 2018, Section 9.1, Paragraph two, Clause 2 of this Law shall not be applied when deciding on the issuing of the facility security clearance to a merchant, but the condition that the merchant must be registered at least one year ago shall be met.

[*1 February 2018*]

12. A person to whom the personnel security clearance has been issued until 30 June 2018 in accordance with Section 9, Paragraph five of this Law shall be allowed access to an official secret until the end of the term of the personnel security clearance, unless other basis for the cancellation of the personnel security clearance laid down in this Law exists.

[*1 February 2018*]

13. Deletion of Section 9, Paragraph eight and Section 11, Paragraph seven of this Law shall come into force on 1 January 2024.

[*20 April 2023*]

14. Each institution shall, by 31 December 2023, review and update the list of information for official use only and the information which has been given the status “dienesta vajadzībām” [information for official use only] in accordance with the Freedom of Information Law, following the provisions of this Law. Until 31 December 2023, the availability and protection of information which has been given the status “dienesta vajadzībām” [information for official use only] in accordance with the Freedom of Information Law shall be ensured in accordance with the regulatory framework of the Freedom of Information Law that was in force until 30 April 2023.

[*20 April 2023*]

The Law shall come into force on 1 January 1997.

The Law has been adopted by the *Saeima* on 17 October 1996.

President G. Ulmanis

Rīga, 29 October 1996