

Translation from Finnish

Legally binding only in Finnish and Swedish

Ministry of Justice, Finland

Security Clearance Act

(726/2014; amendments up to 965/2020 included)

By decision of Parliament, the following is enacted:

Chapter 1

General provisions

Section 1

Objective of the Act

The objective of this Act is to facilitate the prevention of activities that may harm national security, national defence, Finland's international relations, public security or other similar public interests, or highly significant private economic interests or security arrangements introduced to protect the interests referred to above.

Section 2

Scope of application of the Act and its relationship with other legislation

This Act contains provisions on

- 1) the prerequisites for conducting security clearances and on the procedures used in the process;
- 2) information used in the conducting of security clearances;
- 3) consent of the persons subject to the security clearance and on their right of access to information;
- 4) obligation of the applicant for a security clearance and the person subject to a security clearance to provide information;

5) validity of the security clearance and the certificate issued on the basis of the security clearance and on revoking the certificate;

6) combining data contained in personal data files to monitor the integrity and reliability of the person subject to a security clearance and on the measures arising from this. (347/2020)

Separate provisions are issued on an employer's right to collect and retain information on a job applicant or a person that has applied for a public office or a person in an employment relationship with this employer, on checking the criminal record of persons working with children and on checking the criminal record of a person as part of the issuing of an official permit or granting of official approval.

Provisions on the processing of personal data by the Finnish Security and Intelligence Service and the Defence Command are laid down in the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). Provisions on the processing of personal data by other public authorities are laid down in the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and in the Data Protection Act (1050/2018). (347/2020)

Section 3

Definitions

For the purposes of this Act,

1) a personnel security clearance means a report on a person's background prepared in the manner laid down in this Act to ensure the integrity or reliability of the person in question;

2) a facility security clearance means a report prepared in the manner laid down in this Act to determine the reliability of a company and the persons in charge of its operations, the level of information security in the company and the company's ability to meet its commitments;

3) a security clearance means a personnel security clearance and a facility security clearance;

4) a party subject to a security clearance means a person or a company on which a security clearance has been requested;

5) an authority means an organisation, body or a person referred to in section 4 of the Act on the Openness of Government Activities (621/1999);

6) a company means a natural person or other unit carrying out business activities that under section 3, subsection 1, paragraphs 1–5 of the Business Information Act (244/2001) must be registered in the Business Information System;

7) a person in charge of a company means a person who is entered in a public register of an authority as a partner, general partner, managing director, member or deputy member of the company's board of directors, or as a person with procuration rights and the right to sign for the company;

8) an employer means an authority or a company that is considering a person for a service relationship or with which a person is in a service relationship;

9) a close family member means the father, mother, spouse or cohabiting partner of a party subject to a security clearance;

9a) foreign interests mean the citizenships of a party subject to a security clearance at the time of and prior to the security clearance, his or her actions in the service of another country, his or her participation in business activities in another country, assets held by him or her in another country, his or her close family members that are citizens of another country, his or her continuous and close links with citizens of another country, and his or her other interests concerning another country or its citizens and communities; (949/2017)

10) an international information security obligation means a requirement and a security arrangement observed in the ensuring of information secure processing of a confidential document contained in an international agreement or a legal provision that is binding on Finland;

11) a classified document means a document referred to in section 5, subsection 1 of the Act on the Openness of Government Activities, which has been marked as a security classified document under the Act on Information Management in Public Administration (906/2019) or provisions

issued under it or under the Act on International Information Security Obligations (588/2004) to show which information security requirements shall be observed in the processing of the document. (910/2019)

The provisions of subsection 1, paragraph 6 concerning a company and provisions of paragraph 7 concerning a person in charge of a company also apply to foundations or associations that do not carry out business activities and the members of the boards of directors of such foundations and associations, and the persons that under the Finnish Register of Foundations or the Finnish Register of Associations have the right to sign for the foundation or the association.

The provisions of this Act concerning confidential or classified documents also apply to information that has been obtained orally or that can be obtained by making observations if the documents containing such information were confidential or could be classified under the provisions referred to in subsection 1, paragraph 11. (910/2019)

Chapter 2

Position and rights of the party subject to a security clearance

Section 4

Notification of the security clearance

The party that intends to apply for a personnel security clearance on a person considered for a service relationship or a task must state its intention in a notification of a vacant public office or a task or in another appropriate manner. The same applies to a training organiser if there is an intention to request a personnel security clearance on a person considered for the training.

The party that intends to apply for a facility security clearance on a party with whom it intends to conclude a purchase contract must include a notification in the contract notice or the invitation to tender stating that a facility security clearance will be conducted. If the contract is not a contract referred to in the Act on Public Defence and Security Contracts (1531/2011), the notification can also be given by other means.

The provisions of subsections 1 and 2 do not apply if the party subject to the security clearance is applying for the security clearance.

Section 5

Consent of the party subject to the security clearance

A general prerequisite for conducting a security clearance and the monitoring of reliability in connection with the security clearance referred to in section 51 is that the party subject to the security clearance has given prior written consent to the security clearance and the monitoring of reliability.

It must be stated in the consent document that before giving consent, the party subject to the security clearance has been provided with details of the purpose of the security clearance and the monitoring of reliability, of the use of the security clearance and the monitoring of reliability, data processing pertaining to the security clearance and its monitoring and the party's right to be informed of the contents of the security clearance.

The consent to a personnel security clearance can apply to all situations in which a personnel security clearance must be conducted during the service relationship or task specified in the consent or on the basis of which a personnel security clearance certificate must be issued. The consent may also apply to all tasks in a specific administrative branch.

If the party subject to a security clearance applies for the security clearance, a notification of the party subject to the security clearance must be submitted instead of the consent document. The notification must contain the information referred to in subsection 2.

Section 6

Right to be notified of the security clearance

Everybody has the right to be notified by a competent authority whether a security clearance has been conducted on him or her or on the company that he or she has the right to represent. The party subject to the security clearance has the right to receive, on his or her request, the information contained in the security clearance from a competent authority.

The applicant for the security clearance must notify the party subject to the security clearance of the end result of the security clearance. If the security clearance has been issued in writing, the security clearance must also be made available for viewing or, when requested, as a copy.

The provisions of subsections 1 and 2 do not apply if the information has been obtained from a personal data file that the data subject does not have the right to inspect under the law.

If the competent authority refuses to make the information available, it must provide the reasons for its refusal in the written decision given to the party requesting the information.

Section 7

Right of the party subject to the security clearance to submit comments

The party subject to a personnel security clearance has the right to submit comments on the matters that have become known in connection with the interview or the checking of the information entered in the personal data form referred to in section 28.

The competent authority must make an entry on the comments submitted by the party subject to the security clearance in the personnel security clearance conducted on the party subject to the security clearance unless the information is immediately corrected on account of the comments or unless the comments must be considered manifestly unjustified.

If the competent authority refuses to make an entry on the comments in the personnel security clearance it must give the reasons for this in the written decision given to the party subject to the security clearance.

Subsection 4 was repealed by Act 347/2020.

Section 8

Applying the provisions to close family members

The provisions of this chapter concerning the consent of the person subject to a security clearance, and his or her right of access to information and right to submit comments also apply to a close family member of the person subject to the security clearance if a security clearance is conducted on this close family member under section 29.

Chapter 3

Competent authorities and the steering of their discretionary powers

Section 9

Competent authorities

The decision on the conducting of a personnel security clearance and a facility security clearance shall be made by the Finnish Security and Intelligence Service unless the decision on the conducting of the security clearance is made by the Defence Command under subsection 3. Liaison officers designated by the Defence Command may work in the Finnish Security and Intelligence Service in tasks referred to in this Act. (931/2016)

Subsection 2 was repealed by Act 931/2016.

The decision on the conducting of a personnel security clearance shall be made by the Defence Command if the person subject to the security clearance works or intends to work in the Finnish Defence Forces or he or she is carrying out a task given by the Finnish Defence Forces or if the security clearance pertains to the operations or purchases of the Finnish Defence Forces. The Defence Command shall decide on the conducting of facility security clearances on companies that manage or intend to manage tasks given by the Finnish Defence Forces or on companies that are connected with purchases of the Finnish Defence Forces. The Defence Command may assign the task of checking the register data required for conducting the security clearance to a unit of the Finnish Defence Forces under its supervision and provide the unit in question with access to the registers used in the checks. The Defence Command may also authorise the unit referred to above to notify the unit of the Finnish Defence Forces applying for the personnel security clearance that the register data does not contain any information that would be negative in terms of the reliability of the person in question.

The Finnish Transport and Communications Agency shall prepare a report on the level of information security in information systems and telecommunications arrangements as part of the facility security clearance. (347/2020)

Notwithstanding the provisions above, competent authorities may, on a case-by-case basis, decide that one of the authorities will conduct the security clearance or part of it instead of another authority or issue a certificate on their basis.

Section 10

Discretion of an authority in accepting a security clearance matter for consideration

Unless otherwise warranted by specific reasons, no security clearance shall be conducted if a similar security clearance has been conducted on the party subject to the security clearance and this security clearance is still in effect.

If there are statutory provisions on the obligation to obtain a security clearance or a certificate issued on the basis of it, the security clearances shall be conducted in accordance with the resources available to the competent authority and considering the following:

- 1) the need to meet international information security obligations;
- 2) the general relevance of the security clearance subject to the application to ensuring information security in public administration or to protecting critical functions of society or highly important private interests;
- 3) equal treatment of the applicants for and the parties subject to the security clearance.

Section 11

Considering certain matters pertaining to the party subject to the security clearance in the conducting of the personnel security clearance

If it emerges during the conducting of a personnel security clearance that the party subject to the security clearance has been sentenced to a punishment by a legally valid decision or his or her punishment has been waived under chapter 3, section 4, subsection 1 or 2 of the Criminal Code of Finland (39/1889), the competent authority must give particular consideration to the following when considering the end result of the security clearance:

- 1) the time passed since the acts in question;
- 2) the age of the person subject to the security clearance when the acts were committed;

3) repeated nature of the acts and the disregard for the rights of other people or the lack of consideration shown by the perpetrator when committing the acts;

4) severity of the punishment;

5) nature of the acts or their significance in relation to the task used as a basis for the security clearance.

The provisions of subsection 1 also apply when the information on the decisions made by the police on the person subject to the security clearance or the measures concerning him or her are evaluated.

When considering the significance of the foreign interests of the person subject to the security clearance with regard to the end result of the security clearance, the competent authority must in particular consider the following:

1) significance of the foreign interests with regard to the task used as a basis for the security clearance;

2) nature, duration and continuity of the foreign interests;

3) the likelihood that the foreign interests will make the person subject to the security clearance vulnerable to exploitation, pressure, bribery or other inappropriate influencing;

4) the likelihood that the foreign interests can, in a manner other than that referred to in paragraph 3, endanger the chances and ability of the person subject to the security clearance to meet the obligations included in the task used as a basis for the security clearance in an independent and in an otherwise reliable manner.

(949/2017)

Provisions on restrictions on using the information in certain cases are laid down in section 32.

(949/2017)

Section 12

Security Clearance Board

The Government appoints a Security Clearance Board, which operates under the auspices of the Ministry of Justice as a body considering security clearance matters, and the ministry responsible for the general steering of information security in public administration as well as the defence administration, foreign affairs administration and other administrative branches playing a key role in the protection of public interests, trade unions, business operators and the required judicial expertise are represented in the board.

The task of the Security Clearance Board is to consider and present general recommendations for interpretations on the following so that it can support the decision-making of competent authorities and promote uniform and consistent interpretation practice:

- 1) tasks on which a security clearance can be conducted considering the prerequisites laid down in the law;
- 2) how the significance of different types of information on an act should be evaluated with regard to the management of different tasks and the need to interview the person subject to the security clearance when the matter is considered;
- 3) matters that may influence the issuing of the security clearance certificate;
- 4) revocation of the security clearance and the security clearance certificate issued on the basis of the security clearance;
- 5) other measures to ensure uniform and equal treatment of the applicants for and parties subject to the security clearance in the security clearance procedure.

In addition to the provisions of subsection 2, the task of the Security Clearance Board is also to submit an opinion to the Finnish Security and Intelligence Service on the application referred to in section 22.

Section 13

Cooperation between competent authorities

Competent authorities must cooperate to create a uniform way to present the security clearance and the certificate issued on the basis of it and a uniform application practice based on the recommendations of the Security Clearance Board.

Chapter 4

Personnel security clearance

Levels of personnel security clearance

Section 14

Standard, comprehensive and concise personnel security clearance

The personnel security clearance shall be conducted on a concise, standard or comprehensive basis as laid down in this chapter below.

Applying for a personnel security clearance

Section 15

Parties that have the right to apply for a personnel security clearance

Unless otherwise provided in international information security obligations or unless otherwise laid down in the law, an application for a personnel security clearance can be submitted by the employer of the person subject to the security clearance or the party assigning the task that the person subject to the security clearance is intended to perform or is performing. If the person subject to the security clearance is a person considered for training, the application for the security clearance shall be submitted by the party organising the training.

A personnel security clearance can also be conducted at the request of a party other than the applicant referred to in subsection 1 if the security clearance is required under the rules of an international organisation or body or under the law of another country or if it is required so that person subject to the security clearance

- 1) can be selected to perform tasks in an international organisation or body or in another country;
- 2) can start business activities in another country.

Section 16

Obligation of a central government authority to apply for a personnel security clearance

It can be laid down by Government decree that a central government authority must obtain a personnel security clearance on a person that has the right to process, other than on an occasional basis, security class I or II documents or other confidential documents if the unlawful disclosure or unlawful use of the confidential information contained in these documents can cause particularly significant harm to the public interest referred to in the non-disclosure provision or who otherwise manages tasks in which he or she, by disclosing confidential information or by other unlawful means, can significantly harm national security, national defence, international relations, emergency preparedness, civil defence or critical functions of society, or the security arrangements introduced to protect the interests referred to above. (910/2019)

Provisions on requiring a personnel security clearance certificate as a prerequisite for appointment to a public office are laid down in the Act on Public Officials in Central Government (750/1994).

Section 17

Application for a personnel security clearance and the information required for processing the application

The application for a personnel security clearance must be submitted in writing. The consent document referred to in section 5, subsection 2 or, if the person subject to the security clearance is applying for the personnel security clearance, the information referred to in section 5, subsection 4 must be appended to the application.

The following information must be given in the application for a personnel security clearance:

- 1) name and personal identity code of the person subject to the security clearance or, in the absence of a personal identity code, date and place of birth, home municipality, contact details,

citizenship and occupation as well as changes in the name, personal identity code or citizenship of the person in question;

2) the post or task for which the person subject to the security clearance is considered or in which he or she is currently employed;

3) the details of the post or the task that are required when the prerequisites for conducting the security clearance are considered;

4) will the person subject to the security clearance be requested to provide a drug test certificate or undergo a health examination in the manner specified in the law or will his or her credit details be obtained in a manner specified in the law before he or she is selected for the task.

The following information must be appended to the application for a standard or comprehensive personnel security clearance: for the maximum period of ten years preceding the application, details of the places of residence of the person subject to the security clearance and places where he or she has stayed for extended periods and a personnel record or, for the period of at least ten years preceding the application, a record stating the details of the education, training and employment and public service relationships of the person subject to the security clearance. The information contained in the personnel record is not required for a person already employed by a competent authority or its administrative branch if the competent authority in question is able to obtain the information *ex officio*. When an application for a comprehensive personnel security clearance is submitted, the personal data form referred to in section 28 must be appended to the application or the form must be submitted separately.

In addition to the provisions above, the applicant for a personnel security clearance must, at the request of the competent authority, provide information that must be taken into account under this Act when the prerequisites for conducting a personnel security clearance or issuing a personnel security clearance certificate on its basis are considered.

Prerequisites for conducting a personnel security clearance

Section 18

Meeting of security requirements as a general prerequisite

The general prerequisite for conducting a personnel security clearance is that the applicant has by technical and other means restricted access to the information to be protected, ensured the protection of its facilities and information systems and taken other appropriate measures to ensure information security and other security arrangements.

Meeting of the requirement referred to in subsection 1 above can be verified with a certificate issued by an approved evaluation agency referred to in the Act on Information Security Evaluation Agencies (1405/2011), a certificate issued in accordance with the Act on the Evaluation of Government Information Systems and Telecommunications Arrangements (1406/2011), a security plan or in another manner approved by the competent authority deciding on the conducting of the security clearance.

The provisions above do not apply if the personnel security clearance is conducted under section 19, subsection 2, or section 21, subsection 2, or if the party subject to the security clearance carries out tasks referred to in section 43, subsection 1, paragraph 2.

Section 19

Duties falling within the scope of the standard personnel security clearance

A standard personnel security clearance can be conducted on a person considered for a service relationship or a task or a person in a service relationship or a task who

1) is granted the right to process, other than on an occasional basis, official documents that must be classified as security class II or III documents or to otherwise perform tasks in which he or she, by disclosing confidential information or by other unlawful means, can significantly harm national security, national defence, international relations, emergency preparedness, civil defence or critical functions of society, or the security arrangements introduced to protect the interests referred to above; (910/2019)

- 2) performs duties for the Parliamentary Office, Office of the President of the Republic, Parliamentary Ombudsman or the National Audit Office and when performing these duties, can access information comparable to the information referred to in paragraph 1 or is granted a permanent right to enter Parliamentary premises;
- 3) performs tasks directly serving Finland's political leadership in which a particularly high degree of reliability can be required;
- 4) performs tasks in which he or she can harm the infrastructure critical to the functioning of society or the continuation of critical production;
- 5) can, as an information system administrator or taking into account the other powers available to him or her harm the functioning of the information systems critical to the activities of the public authorities or basic functions of society or their information security;
- 6) can, as part of his or her work tasks, access information that when disclosed or otherwise processed by him or her or when he or she is otherwise acting in an unlawful manner, cause serious harm to the national economy, functioning of the financing and insurance systems, or to business activities important to the national interests; (266/2020)
- 7) is responsible for aviation security checks, access control or other security controls or is performing them in security restricted areas at airports or has otherwise unescorted access to security restricted areas at airports as part of his or her work tasks. (266/2020)

A standard personnel security clearance can also be conducted to meet an international information security obligation and, on the application of the person in question, for a task in an international organisation or body as laid down in section 15, subsection 2, or on a person who is considered

- 1) for a task in the defence administration, a study place in the National Defence University, training referred to in the Act on Voluntary National Defence (556/2007), a task in the National Defence Training Association of Finland, or crisis management and peacekeeping tasks performed as an international joint effort, or as a participant in training activities performed as part of crisis management and peacekeeping tasks;

2) for a study place in the Police University College or a task in the Finnish Border Guard;

3) for training the purpose of which is to prepare the participants for tasks in the Finnish foreign affairs administration.

A standard personnel security clearance shall also be conducted on the basis of an application that the Finnish Security and Intelligence Service has accepted for consideration under section 24, subsection 1, or accepted to be processed under section 22.

Section 20

Duties falling within the scope of the comprehensive personnel security clearance

A comprehensive personnel security clearance may only be conducted on a person who

1) as part of his or her work tasks is granted the right to process, other than on an occasional basis, security class I or II documents or other confidential documents containing confidential information that when unlawfully disclosed or used in an unlawful manner can cause particularly significant harm to the public interests referred to in the non-disclosure provision; (910/2019)

2) carries out tasks in which he or she, by disclosing confidential information or by other unlawful means, can harm national security, national defence or Finland's international relations;

3) needs the certificate issued on the basis of the personnel security clearance because of an international information security obligation or in order to qualify for a task in an international organisation or body.

Section 21

Duties falling within the scope of the concise personnel security clearance

A concise personnel security clearance can be conducted on a person considered for a service relationship or a task or a person in a service relationship or a task who

1) is granted the right to process official documents classified as security class III or IV documents or other confidential documents containing confidential information that when unlawfully disclosed

or used in an unlawful manner may cause harm to the public or private interests referred to in the non-disclosure provision; (910/2019)

2) is employed in the production of passports, identity cards or other official certificates in which a particularly high degree of reliability is required;

3) is granted a permanent right to enter an official facility closed to the public and independently perform construction, installation, maintenance or guard tasks or other similar tasks in the facility if the unlawful use of the information about the facility or unlawful acts taking place in the facility may harm public security, national security or other important public interests;

4) may enter premises closed to the public in a port or in a transport area other than an airport that are important for the continuity and security of the country's external or internal transport connections, or premises that are important for the overall functioning of telecommunications or electricity and energy supply; (266/2020)

4a) is working in tasks related to aviation security checks, access control or other security controls outside security restricted areas at airports or is working in tasks in which he or she has unescorted access to air cargo and mail, air carrier mail and air carrier material, in-flight supplies and airport supplies after security controls have been applied to them; (266/2020)

5) is taking part in the transport of nuclear material or nuclear waste or is able to enter a nuclear facility or by entering a nuclear facility construction site or by otherwise taking part in the design or construction of a nuclear facility obtains information on factors relevant to the safety of a nuclear facility or is able to enter a facility in which nuclear material is used or stored or a facility in which a radiation source is used or stored and the amount of the radioactive substances located in the facility corresponds to the radiation level of a high-level sealed source referred to in radiation legislation or is higher; (965/2020)

6) is working in tasks connected to the production or transport of explosives or can otherwise obtain substantial amounts of explosives or other such substances that when inappropriately handled may cause damage in a large area or harm a large number of people;

7) can obtain large amounts of substances that can be used as biological, chemical or toxic weapons;

8) is working in a public utility, food security or medical security task or in a duty supporting these tasks in which he or she can cause serious harm to public health or security;

9) can enter a cash counting facility or is working in cash production, is managing the transport of valuables on behalf of his or her employer or a customer of the employer or is processing large amounts of items of substantial value (such as cash, securities or valuables) in other similar conditions independently and without continuous supervision and no continuous supervision can be arranged for the purpose;

10) on account of his or her position, is granted the right to transfer assets of his or her employer or a customer of the employer or change information on them if the unlawful use of the powers or instructions on using the rights may cause general harm to the reliability of the financial or insurance system or substantial harm to a financial or insurance institution or its customers.

A concise security clearance can also be conducted on a person who

1) is considered for a civilian crisis management task referred to in the Act on the Participation of Civilian Personnel in Crisis Management (1287/2004) or for civilian crisis management training activities;

2) is working in managerial or expert tasks in the administration of the Emergency Response Centre Agency or in on-duty tasks in an emergency response centre, in managerial or expert tasks in the administration of the police or rescue services, or in day-to-day rescue tasks;

3) is considered for training leading to a vocational qualification for rescue services or emergency response centre activities referred to in the Act on the Emergency Services Academy Finland (607/2006), training leading to a university of applied sciences degree for rescue service officers, or for training provided by the Training Institute for Prison and Probation Services;

4) has applied for a charger's certificate or has started security company manager, use of force instructor, weapons instructor, security guard, crowd controller instructor or crowd controller training or training preparing for the tasks of a security officer referred to in the Act on Private Security Services (1085/2015). (1100/2015)

A concise security clearance shall be conducted on persons performing tasks or considered for tasks that the Finnish Security and Intelligence Service has approved for the security clearance procedure under section 22 or tasks that it has moved to the category of concise security clearance matters under section 24.

Section 22

Approving certain tasks as tasks requiring a security clearance

In addition to the provisions of sections 19 and 21, the Finnish Security and Intelligence Service may also, on the application of a company, approve tasks performed in the company or in companies acting on the company's behalf as subcontractors as tasks requiring a standard or concise personnel security clearance, if the person considered for the task or performing it

1) is granted access rights to his or her employer's information system or the information system of a customer of the employer, and the unlawful use of the information system may interrupt or substantially endanger the functioning of the information system so that it will result in an extensive interruption to production activities or in a similar manner cause significant economic harm to the employer or its customer;

2) is granted access to the trade secrets or technological development work of his or her employer or the employer's partners or the use of the results of this work, and the unlawful disclosure, use or other processing of this information will cause significant economic harm to the employer or its customers or partners. (622/2018)

In addition to the provisions of section 18, the following is also required as a prerequisite for a security clearance by the Finnish Security and Intelligence Service:

1) the company, its sector or activities may be targeted for industrial espionage; or

2) the security clearance is required for protecting particularly important private economic interests.

Before making the decision referred to in subsection 1, the Finnish Security and Intelligence Service must request an opinion from the Security Clearance Board on the application submitted by a company to the Finnish Security and Intelligence Service.

Subsection 4 was repealed by Act 931/2016.

Processing a personnel security clearance matter

Section 23

Using and checking register data and interviewing the person subject to a security clearance

The personnel security clearance shall be conducted by checking the register data on the person in question in the manner laid down in this chapter and, if necessary, by carrying out an interview with the party subject to the security clearance in which he or she is asked questions about his or her general circumstances, stay outside Finland, foreign interests and other matters that are particularly relevant when his or her independence and reliability are also evaluated in other respects from the perspective of the task used as a basis for the security clearance. (949/2017)

Notwithstanding non-disclosure provisions, competent authorities have the right to obtain from the other authorities information to ensure that the information obtained from the registers is not out of date or otherwise misleading, and the right to use such information in the conducting of the security clearance.

When a comprehensive personnel security clearance is conducted, the financial position and foreign interests of the party subject to the security clearance and matters concerning his or her close family members can also be examined by conducting a standard personnel security clearance on his or her close family members as laid down in section 25. (949/2017)

Section 24 (931/2016)

Right of the Finnish Security and Intelligence Service to decide on the level of the personnel security clearance

Notwithstanding the provisions of sections 19 and 21, the Finnish Security and Intelligence Service may process an application for a concise personnel security clearance as a matter concerning a standard personnel security clearance if this is necessary to ensure national or public security. For this purpose, the Finnish Security and Intelligence Service may combine the identification details of the party subject to the security clearance contained in the security clearance register referred to

in section 48 with the operational information system of the Finnish Security and Intelligence Service.

The Finnish Security and Intelligence Service may process an application for a standard personnel security clearance as a concise personnel security clearance matter if this is practical and conducting the personnel security clearance in standard form is not required for reasons of national or public security.

Information sources used

Section 25

Information sources for a standard personnel security clearance

A personnel security clearance may only be based on register data contained in the

- 1) Population Information System;
- 2) criminal records, business prohibition register and the register of fines;
- 3) national processing system of the register and case management system of the judicial administration's national information system on criminal cases submitted for consideration of charges or the decisions on criminal cases entered in the decision and reporting system;
- 4) personal data files of the police containing information referred to in section 5, subsections 1 and 2; section 6; section 11; section 12, subsection 1; section 48, subsection 1; and section 49 of the Act on the Processing of Personal Data by the Police (616/2019); (634/2019)
- 5) military justice register and security information register kept by the Defence Command; (340/2019)
- 6) information referred to in section 7; section 8, subsections 1 and 2; and sections 9, 13 and 14 of the Act on the Processing of Personal Data by the Finnish Border Guard (639/2019) and the personal data file of the Finnish Board Guard containing information processed for the purpose of performing surveillance duties referred to in section 15 of the Act; (649/2019)

7) information referred to in section 7, subsections 1 and 2; and section 8 of the Act on the Processing of Personal Data by the Finnish Customs (650/2019); (656/2019)

8) registers of self-employed persons and their operating licences;

9) details of the competence of the persons in charge of companies entered in the registers of the authorities supervising statutory activities;

10) case management system of aliens affairs or the national visa information system and systems containing data on which provisions are laid down in section 7, subsection 1, subsection 2, paragraph 1 or 2, or subsection 4 of the Act on the Processing of Personal Data by the Immigration Administration (615/2020), to the extent that the matter concerns personal data of the family members, persons living in the same household and recipients living in Finland referred to in subsection 1, or 2, paragraph 1 or 2 of the said section, or in section 8; (623/2020)

11) enforcement register and the credit information register;

12) registers corresponding to the registers referred to in paragraphs 1–3 above maintained by the authorities of other countries;

13) data in the registers corresponding to the registers referred to in paragraph 4 above maintained by the authorities of other countries if

- a) the information corresponds to the information that can be entered in the register referred to in paragraph 4 above;
- b) the information has been obtained from another European Union Member State or on the basis of an international information security obligation or from a register kept by the authorities of another country corresponding to the requirements referred to above; and
- c) if the information is entered in a personal data file kept by a competent authority.

When a standard personnel security clearance is conducted, a notification provided by the National Bureau of Investigation based on the information on personal categories kept in the personal data file of the police and referred to in section 7, subsection 2 of the Act on the Processing of Personal Data by the Police can be used. The notification must contain the details that are required by the

Finnish Security and Intelligence Service to evaluate the relevance of the information. The National Bureau of Investigation can submit the notification if

1) the information referred to in section 8 of the Act on the Processing of Personal Data by the Police indicates that there are recurring and permanent links between the person subject to the security clearance and a person that according to a court decision has taken part in the activities of an organised criminal group or according to an ongoing criminal investigation or consideration of charges is suspected to have taken part in such activities, if the links are likely to make the person subject to the security clearance vulnerable to inappropriate external influence and in this way endanger the protection of the interest used as a basis for the security clearance;

2) the National Bureau of Investigation is of the view that on the basis of the information referred to in section 8 of the Act on the Processing of Personal Data by the Police and any other investigations, there are justified reasons to suspect that the person subject to the security clearance has taken part in the activities of an organised criminal group and relaying the information is essential for protecting the interests used as a basis for the security clearance against the activities or influence of an organised criminal group or for preventing an offence; or

3) the information referred to in section 8 of the Act on the Processing of Personal Data by the Police contains entries on evaluating the reliability of the person that are important in terms of quality and contents, and based on these entries the National Bureau of Investigation is of the view that there are justified reasons to suspect that the person subject to the security clearance may endanger the protection of the confidential documents and the information contained in them that he or she can access in his or her work tasks prompting the security clearance that are classified as security class I or II documents, or the unlawful disclosure of the confidential information contained in the documents can otherwise cause particularly significant harm to the public interest referred to in the relevant non-disclosure provision and that the person subject to the security clearance may thus promote the activities of an organised criminal group, if relaying the information is essential for protecting key government security interests against the actions or influence of organised criminal groups or for preventing an offence. (910/2019)

(634/2019)

Foreign interests of the person in question may be examined as part of a standard security clearance if the clearance is conducted

1) for a task referred to in section 19, subsection 1, paragraph 1 or to meet an international information security obligation; or

2) on a person considered for

- a) studies in the National Defence University leading to a degree for an officer's post;
- b) studies in the Police University College leading to a qualification for police duties or studies leading to a university of applied sciences degree for rescue services tasks;
- c) studies in the Border and Coast Guard Academy leading to a qualification for a border guard's post; or
- d) training the purpose of which is to prepare participants for tasks in the Finnish foreign affairs administration.

(949/2017)

The foreign interests can also be examined with the consent of the person in question when a competent authority considers it necessary on the basis of the information that has become known during the conducting of the security clearance and on the basis of the task prompting the security clearance. (949/2017)

Section 26

Information obtained from the registers maintained by the authorities in foreign countries

To ensure the comprehensiveness of the security clearance, the party subject to a personnel security clearance who has lived outside Finland for an uninterrupted period of more than five years during the ten years preceding the security clearance may present a certificate of register data referred to in section 25, subsection 1, paragraphs 1–3 issued by the authorities in a foreign country that he or she can obtain for this purpose under the legislation of the country in question.

The provisions laid down in subsection 1 do not apply to

1) obtaining the information from countries from which a competent authority may obtain the information ex officio under an international agreement or legal provision;

2) persons who during the period referred to in subsection 1 have been outside Finland in a service relationship with a company or an authority or with an international organisation or body.

Based on the information that it has accumulated as part of its operations, the Finnish Security and Intelligence Service must, by means of a public information network or by other suitable means, provide details of the competent authorities of other countries that under the legislation of the countries in question are responsible for background checks on persons or maintenance of the registers used for this purpose and their contact details.

Section 27 (949/2017)

Information sources for a comprehensive personnel security clearance

In addition to the provisions of section 25, subsections 1 and 2, the following information on the person subject to the security clearance may also be obtained as part of a comprehensive personnel security clearance:

- 1) details of his or her business activities or participation in business activities;
- 2) details of his or her assets and debts and other economic interests;
- 3) details his or her family relationships;
- 4) details of his or her foreign interests.

Section 28 (949/2017)

Personal data form and checking the information entered in it

The party subject to the security clearance shall submit a personal data notification as a basis for the comprehensive personnel security clearance providing the details of

- 1) his or her business activities during the ten years preceding the security clearance or details of his or her participation in the business activities;
- 2) his or her assets and debts and other economic interests;
- 3) his or her family relationships;

4) his or her foreign interests.

In addition to the provisions of sections 25 and 57, a competent authority may also check the information provided and obtain information for this purpose from

- 1) the public taxation data of the Finnish Tax Administration;
- 2) registers established for public use containing public information describing business activities or assets;
- 3) credit and financial institutions, subject to the permit granted by the party subject to the security clearance;
- 4) a country or an international body from which a competent authority may under an international agreement or legal provision and for the purpose of examining foreign interests obtain information for the security clearance procedure.

The provisions on reporting foreign interests laid down in subsection 1, paragraph 4, and on the information sources available to competent authorities laid down in subsection 2, paragraph 4 also apply when the foreign interests of the party subject to the security clearance are examined as part of a standard personnel security clearance.

The competent authority must provide the party subject to the security clearance with an opportunity to comment on the matters that have become known in connection with the checking of the information that he or she has given.

Section 28a (949/2017)

Notification of the party subject to the security clearance of changes in his or her foreign interests

The person whose foreign interests have been examined as part of the personnel security clearance conducted on him or her must notify the authorities that have conducted the security clearance of new or changed foreign interests without undue delay. There is no obligation to submit the notification if the personnel security clearance or the personnel security clearance certificate issued on its basis is no longer in effect.

Section 28b (949/2017)

Obligation of the competent authorities to provide information concerning changes in foreign interests

If a competent authority considers that the notification submitted by the party subject to a security clearance under provisions laid down in section 28a contains information that might have impacted the issuing of the security clearance certificate or the contents of the end result of the security clearance, the competent authority must, notwithstanding non-disclosure provisions and after hearing the views of the party subject to the security clearance, notify the applicant for the personnel security clearance of the matter.

Before making the notification referred to in subsection 1, the competent authority must examine whether the party subject to the security clearance is still in the service of the employer that applied for the personnel security clearance or employed in the tasks carried out on behalf of the applicant or whether he or she is studying in the education institution that applied for the security clearance or is he or she taking part in training provided by the foreign affairs administration.

Notwithstanding subsection 1, the information on the end result of the monitoring shall be sent to the party that in accordance with section 48, subsection 5 has entered the start of service relationship of the party subject to the security clearance in the security clearance register unless the service relationship has been declared as ended.

Section 29

Extending the personnel security clearance to cover close family members in a comprehensive security clearance

If achieving the objective of the comprehensive personnel security clearance so essentially requires, the personnel security clearance can, on a case-by-case basis, be extended to cover close family members of the party subject to the security clearance.

Section 30

Information sources for the concise personnel security clearance

A concise personnel security clearance shall be conducted using the register data referred to in section 25, subsection 1, paragraphs 1–10, except for the operational information system of the Finnish Security and Intelligence Service and the security information register of the Defence Command.

Section 31

Special provisions applying to the Finnish Defence Forces and the Finnish Security and Intelligence Service

In addition to the provisions of section 25, the Defence Command may also use information that can be obtained from the register of persons liable for military service and the register of crisis management personnel when conducting personnel security clearances on persons considered for or carrying out tasks in the Finnish Defence Forces.

The information on health and eligibility for military service obtained from the register of persons liable for military service may only be considered in the conducting of the security clearance if it is essential for ensuring the personal security of other people.

The provisions on the Defence Command laid down in subsections 1 and 2 also apply to the Finnish Security and Intelligence Service when it conducts personnel security clearances on persons that are considered for tasks in the Finnish Security and Intelligence Service.

Section 32

Restrictions on the use of information in the conducting of a personnel security clearance

The following information may not be used in the conducting of a personnel security clearance:

- 1) denunciations or reports of offences or other similar information supplied to the police claiming that the person in question is reported to have committed or to commit an offence unless the information has led to a criminal investigation;

Paragraph 2 was repealed by Act 634/2019.

3) details of criminal acts committed more than ten years before the conducting of the security clearance unless the information can be obtained from the criminal records;

4) details of acts committed at the age of under 15 years unless using the information is essential for ensuring the personal security of other people in the Finnish Defence Forces.

Information concerning a matter under criminal investigation or under consideration by the prosecutor may only be used if

1) it is examined how far the matter has progressed and the type of the information on the guilt of the party subject to the security clearance is determined;

2) using the information is essential on account of the special requirements concerning the task used as a basis for the security clearance and the nature of the suspected act.

Health information contained in the information referred to in section 5, subsections 1 and 2; sections 6 and 11; section 12, subsection 1; section 48, subsection 1; and section 49 of the Act on the Processing of Personal Data by the Police may only be considered in the conducting of the security clearance if it is essential for ensuring the personal security of other people and the health information is based on a medical certificate or other entries made by approved health care professionals or information that they have provided orally under the law and the accuracy of the information cannot be disputed. Notwithstanding the provisions in this subsection above, a competent authority may draw an employer's attention to the need to carry out measures referred to in section 17, subsection 2, paragraph 4 of this Act. (634/2019)

Chapter 5

Facility security clearance

Section 33

Parties that have the right to apply for a facility security clearance

An application for a facility security clearance can be submitted

1) by a party that needs the security clearance to meet an obligation laid down in the law or an obligation under the law or an obligation arising from an international information security obligation;

2) by an authority that intends to conclude an agreement with the party subject to the security clearance if in connection with the agreement, the company gets access to or the agreement results in documents classified as security class I–III documents or other confidential documents containing confidential information that when unlawfully disclosed or used in an unlawful manner may cause harm to the public or private interests referred to in the non-disclosure provision; (910/2019)

3) in situations referred to in paragraph 2, by a unit responsible for central government procurement or a unit providing central government with information and communications technology services intended for shared or extensive use;

4) by an authority supervising the activities referred to in section 21, subsection 1, paragraphs 5 and 6.

In cases referred to in section 36, subsection 2, the facility security clearance can be conducted at the request of the party subject to the security clearance.

Section 34 (910/2019)

Obligation of a central government authority to apply for a facility security clearance

It may be laid down in a Government decree that a central government authority must obtain a facility security clearance on a company that, in order to implement an agreement with a central government authority, is provided with security class I–III documents or other confidential documents containing confidential information that when unlawfully disclosed or used in an unlawful manner may cause harm to the public or private interests referred to in the non-disclosure provision.

Section 35

Application for a facility security clearance

An application for conducting a facility security clearance must contain the following information:

- 1) name and other identification data and contact details of the party subject to the security clearance;
- 2) details of the subcontractors with whom the party subject to the security clearance intends to conclude an agreement on the carrying out of the project used as a basis for the facility security clearance, role of the subcontractors in the carrying out of the project and the details of the subcontractors referred to in paragraph 1;
- 3) information on the fulfilment of the prerequisites for conducting a facility security clearance laid down in section 36;
- 4) information stating whether the purpose of the facility security clearance is to verify that the company meets a specific level of information security and if so, which evaluation criteria are used;
- 5) information stating whether an approved evaluation agency referred to the Act on Information Security Evaluation Agencies has conducted an evaluation of the facilities, information systems and other security arrangements of the company or its subcontractors and if so, a copy of the certificate issued on the basis of the evaluation.

A document stating the consent of the company to the conducting of the facility security clearance must be appended to the application unless the application is submitted by the company in question.

Section 36

Prerequisites for conducting a facility security clearance

A facility security clearance can be conducted if it is needed to evaluate a company in the following situations:

- 1) the facility security clearance must be conducted or can be conducted under the law or a provision issued under the law or to meet an international information security obligation;

2) an authority is concluding an agreement with the company and in connection with the agreement, confidential documents of the authority are made available to the company; (910/2019)

3) the authority supervising the activities requests a facility security clearance on a company that carries out activities referred to in section 21, subsection 1, paragraph 5 or 6 or is taking part as a subcontractor in a project in which the company in question or its employees have access to the information, facilities or area referred to in the said legal provisions. (931/2016)

A facility security clearance can be conducted if the security clearance is required under the rules of an international organisation or body or under the law of another country or if it is required so that the party subject to the security clearance

1) can be selected to a project organised by an international organisation or body or a project managed by them or a tendering competition organised in another country;

2) can start business activities in another country.

A facility security clearance can also be extended to apply to a company acting as a subcontractor of the party subject to the security clearance to the extent that the prerequisites laid down in subsection 1 are also met as prerequisites applying to the subcontractor and this is considered necessary by the competent authority.

It can be laid down in a Government decree that a facility security clearance can also be conducted to protect trade secrets or information on technological development work of a company that when unlawfully used, processed or disclosed, would cause the company significant economic harm or the protection of which is important with regard to public interest. (622/2018)

Section 37

Information sources used in a facility security clearance

The following information can be used in the conducting of a facility security clearance:

1) information on the company, its owners and the citizenship of the owners if such information is available;

2) information referred to in section 6, subsection 1 of the Act on the Customer Information System of Business Services (240/2007);

3) information on the activities of the company, number of its employees and other matters describing the personnel in general;

4) credit details of the company and the persons in charge of its operations;

5) information on the company's assets from registers established for public use or information available from other public sources or information provided by the company for conducting the security clearance;

6) information from the enforcement register, public information from the tax authorities' information systems, and information on tax receivables or information obtained from insurance institutions on the non-payment of receivables based on statutory insurance policies that under the Act on the Enforcement of Taxes and Public Payments (706/2007) are directly enforceable;

7) information obtained from the case management system of aliens affairs and the national visa information system on which provisions are laid down in section 7, subsection 1, or subsection 2, paragraph 1 or 2 of the Act on the Processing of Personal Data by the Immigration Administration; (623/2020)

8) information from financial and credit institutions submitted by the company or obtained with the consent of the company;

9) information on criminal convictions and conditional fines imposed on the company and offences targeting the company.

In addition to the provisions of subsection 1, paragraph 3, provisions laid down in chapter 4 also apply to the information sources used in the conducting of the personnel security clearances on the persons in charge of the company in the facility security clearance.

The Act on the Customer Information System of Business Services (240/2007) was repealed by the Act on the Customer Information System of Business Services (293/2017).

Section 38

Processing a facility security clearance matter

When a facility security clearance is conducted, the information given in the application, information sources referred to in section 37 and the inspection of the company, its facilities, information systems and telecommunications arrangements are used to determine how the company can ensure the following:

- 1) the information is protected against unlawful disclosure, alteration and destruction;
- 2) unauthorised access to the facilities in which information is processed or other activities used as a basis for the security clearance carried out is prevented;
- 3) the personnel are guided and trained in an appropriate manner.

If the purpose of the facility security clearance is to verify that the company meets a specific level of information security, it must be examined whether the requirements concerning the security level are met.

The facility security clearance can also be conducted on a partial basis if this is required for meeting an international information security obligation or otherwise justified so that the purpose of the facility security clearance can be met.

Section 39

Inspections carried out in connection with the facility security clearance and an authority's right of access to information

The company on which the facility security clearance is conducted must provide the authority conducting the security clearance with the information that is necessary for conducting the security clearance and give the parties conducting the security clearance and inspectors access to its facilities so that the information can be provided.

A competent authority may inspect the security arrangements implemented to protect the company's facilities, information systems and telecommunications arrangements and other security

arrangements to the extent necessary. The inspection may not be carried out in premises used as permanent dwellings.

Section 40

Undertaking given by the company

When conducting the facility security clearance and when preparing the certificate issued on its basis, the competent authority may require that the business operator undertakes to maintain the level of information security and give notification of changes impacting it and grant the authority access to its premises so that the maintenance of the information security level can be supervised and provide information required for the supervision.

Chapter 6

Concluding the security clearance procedure and processing the information obtained in the procedure

Section 41

Conclusion of the security clearance procedure

The applicant shall be notified of the conclusion of the security clearance and its contents in writing or by issuing the security clearance certificate referred to in section 43 or 46 on the basis of the security clearance.

If there is no obligation to issue a security clearance certificate on the basis of the personnel security clearance or if nothing that the authority conducting the security clearance considers important with regard to the reliability of the party subject to the security clearance has become known during the security clearance process, the authority may, notwithstanding subsection 1, orally state this to the applicant for the security clearance.

Section 42

Impacts of the security clearance and its contents

The security clearance is not binding on the party for whom the security clearance has been produced.

A security clearance may only contain information specified as confidential in such a form and to such an extent that in the case in question are necessary to ensure that the purpose of the security clearance is met and it is obvious that disclosing the information does not endanger national security or other public interests referred to in section 1. If references to a pending criminal case are included in a security clearance, it must also be stated how far the case has progressed by the time when the security clearance has been issued.

A personnel security clearance may not contain an official evaluation of the integrity, reliability or suitability of the person subject to the security clearance for a public office or a task.

In connection with the issuing of a personnel security clearance, the competent authority may draw the employer's attention to the need to carry out measures referred to in section 17, subsection 2, paragraph 4.

Section 43

Issuing a personnel security clearance certificate

The competent authority that has conducted the personnel security clearance shall issue a personnel security clearance certificate on the basis of the personnel security clearance if no reasons for not selecting the person in question for the task used as a basis for the security clearance have become known in the security clearance procedure and if the issuing of the security clearance certificate is necessary

1) under a legal provision or a provision issued under the law or because of the task referred to in section 15, subsection 2;

2) to prevent the conducting of unnecessary security clearances when the party subject to the security clearance works as a charger or in maintenance, installation, security guard or in other such tasks in which he or she must, on account of the nature of his or her work tasks, regularly work in such facilities or areas in which all employees must undergo a security clearance.

The national security authority shall issue the personnel security clearance certificate required for meeting international information security obligations as laid down in the Act on International Information Security Obligations.

In the cases referred to in subsection 1, paragraph 2 above, the certificate may also be issued as an identity card. The Finnish Security and Intelligence Service shall determine the form and contents of the identity card after hearing the views of the Defence Command, considering the provisions laid down in section 44.

If a competent authority refuses to issue a personnel security clearance certificate, it must provide the reasons for its refusal in a written decision given to the applicant for the security clearance and the party subject to the security clearance.

Section 44

Contents of the personnel security clearance certificate

The details of the party subject to the security clearance, certificate date, party issuing the certificate and the tasks for which the certificate has been issued shall be entered in the personnel security clearance certificate.

If necessary, the following information shall be entered in the certificate:

- 1) details of the period of validity of the certificate;
- 2) statement confirming that nothing has become known during the security clearance process that would make the person in question ineligible for the task used as a basis for the application;
- 3) details of the security classified documents or other confidential documents that when unlawfully disclosed or used in an unlawful manner may cause harm to the interests referred to in the non-disclosure provision and to which the party subject to the security clearance can be granted access; (910/2019)
- 4) matters required in international information security obligations.

Section 45

Processing the personal data obtained on the basis of the personnel security clearance

The applicant for the personnel security clearance must ensure that the personal data contained in the security clearance can only be processed by persons in whose tasks the data is of essential

importance and that the information contained in the security clearance and the personnel security clearance certificate is only used for the purposes stated in the application. The same applies to those that have obtained a security clearance or a personnel security clearance certificate from the party subject to the security clearance. Notwithstanding the provisions above, the information can be processed when an employer interviews a job applicant unless otherwise provided in section 6, subsection 3.

The applicant must destroy the written notification of the security clearance that he or she has received as soon as it is no longer necessary with regard to the purpose of use given when the application for the security clearance was submitted; the notification must, however, be destroyed within six months of the receipt of the information on the security clearance.

Provisions on the confidentiality of the personnel security clearance and the information contained in it are laid down in section 59.

Section 46

Issuing a facility security clearance certificate

The competent authority that has conducted the facility security clearance shall issue the applicant with a facility security clearance certificate on the basis of the facility security clearance if the company in question meets the information security requirements used as a basis for the security clearance. The certificate shall also be issued to the party subject to the security clearance.

The national security authority shall issue the facility security clearance certificate required for meeting international information security obligations as laid down in the Act on International Information Security Obligations.

If the facility security clearance has only applied to the security of the information systems or telecommunications arrangements, the Finnish Transport and Communications Agency, which has conducted the security clearance, may issue a certificate on the basis of the security clearance.

(347/2020)

If a competent authority refuses to issue a facility security clearance certificate, it must provide the reasons for its refusal in a written decision given to the applicant for the security clearance and the party subject to the security clearance.

Section 47

Contents of the facility security clearance certificate

The following information shall be entered in the facility security clearance certificate:

- 1) details of the party subject to the security clearance and the party issuing the security clearance;
- 2) if specified, details of the period of validity of the security clearance certificate;
- 3) the matters within the scope of the security clearance and used as a basis for the evaluation and the results concerning them;
- 4) if necessary, the security classified documents or other documents that when unlawfully disclosed or used in an unlawful manner can cause harm to the interests referred to in the non-disclosure provision, and the processing requirements of which the company meets; (910/2019)
- 5) matters that are required under the international information security obligation used as a basis for the security clearance.

If the purpose of use of the facility security clearance so requires, a statement confirming that nothing has become known during the security clearance process that would make the company ineligible for the task used as a basis for the application.

Chapter 7

Security clearance register and data processing in connection with it

Section 48

Security clearance register, purpose of the register and entering information in the register (347/2020)

The security clearance register shall be maintained for the purpose of conducting security clearances, avoiding unnecessary security clearances, relaying information between competent

authorities and implementing the monitoring of reliability and integrity of the parties subject to security clearances. (347/2020)

The Finnish Security and Intelligence Service and the Defence Command must without delay enter in the security clearance register details of each application for a security clearance submitted to them, name and other identification data of each party subject to the security clearance, extent of each security clearance and details of the end result of the security clearance procedure or the security clearance certificate and its period of validity and revocation, and details of the employers of the parties subject to the personnel security clearance, if such information is available. The national security authority must save details of the personnel security clearance certificates and facility security clearance certificates that it has issued and that are required under an international information security obligation. (347/2020)

Notwithstanding the provisions above, the Finnish Security and Intelligence Service can enter details of its own personnel or the Defence Command can enter details of the Finnish Defence Forces personnel in the register to the extent necessary so that they are not available to third parties if making such information available to third parties can endanger the activities of an authority and the carrying out of the tasks falling under its purview.

The Finnish Transport and Communications Agency may enter in the security clearance register the details of

- 1) the certificates that it has issued under the Act on the Evaluation of Government Information Systems and Telecommunications Arrangements and the information entered in them;
- 2) the evaluation agencies approved under the Act on Information Security Evaluation Agencies;
- 3) the certificates issued by an approved evaluation agency as laid down in the Act on Information Security Evaluation Agencies.

(347/2020)

The party that has decided to employ in a service relationship a person and has obtained the details of the personnel security clearance conducted on this person from the security clearance register under section 50, subsection 2, must notify the Finnish Security and Intelligence Service of its decision. A similar notification must also be submitted of the end of the service relationship

referred to above. The notification can be submitted by entering the details in the security clearance register or otherwise electronically in a manner approved by the Finnish Security and Intelligence Service. (949/2017)

The national security authority and the Finnish Transport and Communications Agency must ensure that the information that they have entered in the security clearance register correspond to the decisions taken by an authority and the entries that it has made in its own registers and that the entries have been made in accordance with the technical requirements set by the Finnish Security and Intelligence Service. (347/2020)

Section 48a (347/2020)

Controllers

The Finnish Security and Intelligence Service and the Defence Command shall act as the joint controllers of the security clearance register. The Defence Command shall be responsible for the tasks of the controller if the personal data to be processed concerns a party subject to the security clearance that works or intends to work in the Finnish Defence Forces or that carries out a task given by the Finnish Defence Forces or if the security clearance is connected with the operations or purchases of the Finnish Defence Forces. The Finnish Security and Intelligence Service shall be responsible for the tasks of the controller if the personal data to be processed concerns other parties subject to the security clearance, and for the tasks concerning the disclosure of personal data from the security clearance register and maintenance and information security of the security clearance register.

Section 49 (347/2020)

Removing data from the security clearance register

By derogation from section 6, subsection 3 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security, the information entered in the security clearance register shall be removed no later than three years from the conducting of a corresponding new security clearance or the expiry of the security clearance or security clearance certificate or from the date on which the task for which the security clearance has been conducted has ended or when the security clearance certificate was revoked.

Section 50

Disclosing information from the security clearance register

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service shall disclose information contained in the security clearance register to the Defence Command using a technical interface. The Defence Command can, in a manner approved by the Finnish Security and Intelligence Service, relay to the public officials designated by the units of the Finnish Defence Forces information that is required for evaluating the need for obtaining a security clearance or for processing the permission to access or visit referred to in section 15 of the Act on the Defence Forces (551/2007). (931/2016)

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service may, in a manner approved by it using a technical interface, disclose to a public official designated by the Office of the President of the Republic, Parliamentary Office, a ministry, or an agency in the administrative branch of the Ministry of the Interior information from the security clearance register for evaluating the obtaining of the security clearance that concern (931/2016)

- 1) a company on which a facility security clearance has been conducted and the certificate issued on the basis of the security clearance;
- 2) a personnel security clearance according to which nothing negative on the reliability of the person in question has become known or on the basis of which a certificate has been issued that is still valid;
- 3) a certificate granted for an official information system or official telecommunications arrangements and other information referred to in section 48, subsection 4;
- 4) in cases referred to in paragraphs 1–3, the party conducting the security clearance, the date on which the security clearance was conducted and the period of validity of the certificate.

Notwithstanding non-disclosure provisions, the Finnish Security and Intelligence Service can, using a technical interface, provide the National Bureau of Investigation with the information on applying for a security clearance so that the information can be combined with information on personnel groups referred to in section 7, subsection 2 of the Act on the Processing of Personal Data by the Police for making the notifications referred to in section 25, subsection 2 of this Act and for

consideration concerning it. The National Bureau of Investigation must destroy the information obtained through the combination immediately after the need for making the notification has been evaluated or the notification has been sent to the Finnish Security and Intelligence Service. (347/2020)

Using a technical interface, in cases referred to in subsection 2, information may only be retrieved of persons or companies that have given their consent to the conducting of the security clearance and that are considered for a service relationship or for a task falling within the scope of the security clearance procedure under this Act or of persons for which the processing of a permission to access or visit is pending in a Finnish Defence Forces unit referred to in subsection 1.

The provisions laid down in the Act on International Information Security Obligations apply to the disclosure of personal data to the national security authority. (347/2020)

Section 51

Monitoring of integrity and reliability by combining information contained in personal data files (347/2020)

The Finnish Security and Intelligence Service can combine the information kept in the security clearance register with information referred to in section 5, subsections 1 and 2 and section 6 of the Act on the Processing of Personal Data by the Police and details of pending criminal cases and decisions on criminal cases contained in the judicial administration's national information system to determine whether the security clearance or the certificate issued on its basis can remain in effect. The information can also be combined with the information contained in the notification referred to in section 25, subsection 2, and information referred to in section 48, subsection 1 and section 49 of the Act on the Processing of Personal Data by the Police if the security clearance subject to the examination has been conducted on the basis of section 19, subsection 1, paragraph 7. (266/2020)

The information on a person on whom a comprehensive personnel security clearance has been conducted may be combined with information from personal data files from which, under section 28, subsection 2, information can be retrieved to check information entered on personal data forms.

The Finnish Security and Intelligence Service must destroy the information resulting from the combination immediately after the measures referred to in section 52 have been completed but no later than one year from the combination of the registers. The combined information may only be used or disclosed in cases laid down in section 52 or to process a decision and a request for review made on its basis.

Provisions on the consent to combination of the register data required from the party subject to a security clearance are laid down in section 5.

Section 52

Measures prompted by the monitoring

If on the basis of the monitoring referred to in section 51, it emerges that a person or a company or a person in charge of the company is suspected of a criminal act or by a court decision is considered to have committed a criminal act, the Finnish Security and Intelligence Service must, notwithstanding non-disclosure provisions, report the matter to the authority that has conducted the security clearance.

If based on the information obtained in the monitoring, the person is suspected of an act or by a court decision is considered to have committed an act that could have impacted the issuing of the security clearance certificate or the contents of the security clearance, a competent authority must, notwithstanding non-disclosure provisions and after hearing the party subject to the security clearance, report the matter to the applicant for the security clearance or the ministry that in accordance with section 48, subsection 5, has entered in the register that the party subject to the security clearance has started work in a service relationship unless the service relationship has been declared as ended. Notwithstanding non-disclosure provisions, the competent authority must also disclose the information that is essential for preventing a serious threat to national security and information contained in the notification referred to in section 25, subsection 2, according to which there are justified reasons to suspect that the person in question has taken part in the activities of an organised criminal group or is promoting the activities of an organised criminal group. Before the information is disclosed, it must be clarified with the applicant whether the party subject to the security clearance is still employed by the employer in question or in the tasks assigned to him or her by the client or whether he or she is studying in the education institution that acted as the applicant. (266/2020)

If the information referred to in subsection 2 applies to a person in charge of a company or a company and it would have impacted the issuing of the facility security clearance certificate, the competent authority must, notwithstanding non-disclosure provisions and after hearing the party subject to the security clearance, report the matter to the applicant for the facility security clearance. (266/2020)

If the security clearance certificate has been issued to meet international information security obligations, the national security authority responsible for implementing international information security obligations must be notified of the matters referred to in subsection 1 without delay.

When measures are considered and when subsections 1–4 are applied in the evaluation of the significance of the information concerning the suspected offence and the criminal act, consideration must be given to provisions on the considering of different types of information when the security clearance is conducted laid down in section 32 and elsewhere in the Act.

By derogation from subsections 2 and 3, it is not necessary to hear the person subject to the security clearance concerning a matter of which he or she does not have any right to be informed under section 11 or 12 of the Act on the Openness of Government Activities. (266/2020)

Chapter 8

Period of validity of the security clearance and the security clearance certificate

Section 53

Period of validity of the security clearance and the security clearance certificate

A security clearance is in effect until further notice, but not more than five years. The same applies to the certificate issued on the basis of the security clearance unless the certificate has been issued for a fixed-term task or a task connected to a specific project or the competent authority decides otherwise on account of the special circumstances connected with the security clearance.

Section 54

Renewing the security clearance and issuing a new security clearance certificate

A security clearance issued until further notice may, at the initiative of the authority that conducted the security clearance or on the application of the applicant for the security clearance or

the party subject to the security clearance, be renewed if this is necessary to meet an international information security obligation or because of a change in the tasks or circumstances of the party subject to the security clearance that under this Act shall be considered in the conducting of the security clearance.

A personnel security clearance certificate can be issued on the basis of the information kept in the security clearance register without conducting a new security clearance unless otherwise provided by the monitoring carried out in accordance with section 51.

Section 55

Revoking the security clearance certificate

A competent authority may at its own initiative, or on the application of the applicant for the security clearance, the employer of the party subject to the security clearance or the party subject to the security clearance revoke the personnel security clearance certificate issued under this Act if

1) the party subject to the security clearance is no longer employed in the tasks for which the certificate was issued;

2) according to a notification received on the basis of an international information security obligation, the party subject to the security clearance has failed to comply with the information security requirements binding on him or her in the task for which a personnel security clearance certificate has been issued for him or her in Finland;

3) on the basis of the monitoring carried out in accordance with section 51, the party subject to the security clearance is suspected of an act that would have prevented the issuing of the security clearance certificate or, because of other changed circumstances, he or she could no longer be issued with a security clearance certificate.

The facility security clearance certificate can be revoked if the activities of the company subject to the security clearance are no longer in accordance with the requirements that have been the prerequisite for issuing the security clearance certificate or if a person in charge of the company is suspected of an act referred to in subsection 1, paragraph 2 and the company has not corrected the deficiencies referred to above within the deadline set.

Before making the decision referred to in subsection 1 or 2, the competent authority must hear the party subject to the security clearance and, if necessary, the applicant for the security clearance or the employer of the party subject to the security clearance.

In its decision to revoke the security clearance certificate, the competent authority may order that the decision must be complied with notwithstanding the request for review unless otherwise ordered by the reviewing authority.

Chapter 9

Miscellaneous provisions

Section 56 (347/2020)

Section 56 was repealed by Act 347/2020.

Section 57

Authorities' right of access to information

Notwithstanding the provisions on the non-disclosure obligation laid down in the law,

- 1) the authorities must disclose to the authorities that are competent under this Act the information that they can use in the conducting of a security clearance or in the carrying out of the monitoring in connection with the security clearance;
- 2) competent authorities must disclose to each other information available under this Act for conducting a security clearance.

A competent authority has the right to obtain information from a party maintaining a credit information register for conducting a personnel security clearance and a facility security clearance and when the monitoring referred to in section 51 is carried out.

The information referred to in subsections 1 and 2 above can also be disclosed by means of a technical interface.

Section 58

Notification obligation of the employer and the company that has been issued with a facility security clearance certificate and their obligation to take action

The employer on whose application a personnel security clearance has been conducted on an employee or a personnel security clearance certificate issued on its basis, must notify the authority that conducted the personnel security clearance or issued the personnel security clearance certificate of the end of the service relationship.

If the personnel security clearance certificate has been revoked, the employer on whose application the personnel security clearance certificate has been issued must ensure that the personnel security clearance certificate is returned to the authority that issued the certificate.

If the facility security clearance certificate has been revoked, the company subject to the security clearance must return the facility security clearance certificate to the authority that issued the certificate.

Section 59

Non-disclosure obligation

Sections 22–24 of the Act on the Openness of Government Activities also apply to the non-disclosure obligation and prohibition of use of the party that has obtained information under the law in a matter concerning a security clearance if the documents and the information have been obtained by a party other than the authority referred to in section 4 of the said act.

In addition to the provisions of subsection 1, the company issued with a facility security clearance certificate, persons in charge of the company, persons employed by the company and persons carrying out tasks on behalf of the company must keep secret the information that they have obtained on the basis of the task for which the facility security clearance certificate has been issued or presented.

Section 60 (347/2020)

Fees charged for a security clearance

The applicant shall be charged a fee for the security clearances conducted by competent authorities under this Act and for the expert tasks carried out by the Finnish Transport and Communications Agency in the conducting of the facility security clearance as laid down in the Act on Criteria for Charges Payable to the State (150/1992). However, the party subject to the security clearance shall be responsible for the costs connected with the conducting of the facility security clearance if the security clearance has been conducted on the application of an authority.

Section 61 (347/2020)

Reference to penal provisions

Provisions on the punishment for a data protection offence are laid down in chapter 38, section 9 of the Criminal Code. Provisions on the punishment for a violation of the secrecy of communications are laid down in chapter 38, section 3, for an aggravated violation of the secrecy of communications in chapter 38, section 4, for unlawful access to an information system in chapter 38, section 8, and for aggravated unlawful access to an information system in chapter 38, section 8a of the Criminal Code. A punishment for violating the non-disclosure obligation laid down in section 59 of this Act shall be imposed under chapter 38, section 1 or 2 of the Criminal Code, unless the act is punishable under chapter 40, section 5 of the Criminal Code or a more severe punishment for the act is provided elsewhere by law. Violation of the undertaking referred to in section 40 of this Act is also considered a violation of the non-disclosure obligation referred to above.

Section 62

Request for review

A request for a review of a decision made by a competent authority under this Act may be submitted to an administrative court. Provisions on submitting a request for review to an administrative court are laid down in the Administrative Judicial Procedure Act (808/2019).
(347/2020)

No request for review can be submitted on a decision made by a competent authority under which the conducting of a security clearance is refused or a decision made by the Finnish Security and

Intelligence Service in a matter referred to in section 22. A review on a decision under which the issuing of a security clearance certificate is refused may only be requested if the security clearance certificate is, by law or under a provision issued under the law, a prerequisite for selection for a public office or a task or for carrying out a public office or a task for which a security clearance certificate is required under an international information security obligation.

A review of a decision on the issuing and revocation of a security clearance certificate can be requested by the applicant for the security clearance and the party subject to the security clearance.

The authority whose decision has been repealed or changed by an administrative court may request a review of the administrative court decision to ensure uniform application of the law.

Chapter 10

Transitional provisions and entry into force

Section 63

Entry into force

This Act enters into force on 1 January 2015. This Act repeals the Act on Background Checks (177/2002).

Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.

Section 64

Transitional provisions

The Act in force at the entry into force of this Act shall apply to the matter initiated before the entry into force of this Act. The security clearance register referred to in section 48 of this Act and the information processing carried out in connection with it must be made to comply with the law within two years of the entry into force of the Act.

The details of the security clearances issued under the Act on Background Checks (177/2002) and certificates issued under the Act on International Security Obligations that have been issued no

earlier than three years before the entry into force of this Act may be transferred to the security clearance register.

Before the security clearance register has been made to comply with the law, competent authorities may also, notwithstanding non-disclosure provisions, disclose to each other electronically or otherwise process information on the security clearances and certificates referred to in subsection 2 that are required for meeting the obligation laid down in section 10 of this Act.