Translation from Finnish
Legally binding only in Finnish and Swedish
Ministry of Finance, Finland

Act on Information Management in Public Administration

(906/2019)

"Public Information Management Act"

By decision of Parliament, the following is enacted:

Chapter 1
General provisions

Section 1
Objectives of the Act

The objectives of this Act are:

1) to ensure harmonised and high-quality management and data secure processing of datasets of authorities to implement the principle of openness;

2) to enable secure and efficient exploitation of the datasets of authorities so that an authority may attend to its tasks and provide its services to public administration clients successfully and in a qualitative manner in compliance with good governance;

3) to promote the interoperability of information systems and information pools.

This Act implements, in part, Directive 2013/37/EU of the European Parliament and of the Council amending Directive 2003/98/EC on the re-use of public sector information.

Section 2
Definitions

In this this Act:

1) *an authority* means the authorities referred to in section 4, subsection 1 of the Act on the Openness of Government Activities (621/1999);

2) *an information management entity* means an authority whose task is to arrange information management in accordance with the requirements of this Act;

3) *an information system* means an overall arrangement comprising data processing equipment, software and other data processing;

4) *a document* means an official document referred to in section 5, subsection 2 of the Act on the Openness of Government Activities;

5) *dataset* means an information entity composed of documents and other corresponding information related to a specific task or service of the authorities;

6) *an information pool* means an entity containing datasets used by the authorities in performance of their tasks or for their other activities that is processed through information systems or manually;

7) *a shared information pool* means an information pool designed and maintained for several actors, the information in which can be disclosed and exploited for different purposes;

8) *information security measures* mean the administrative, functional and technical measures to ensure the availability, integrity and confidentiality of datasets;

9) *information management* means the actions based on the needs arising from the performance of the tasks of the authorities or from their other activities and information security measures for managing the datasets of authorities, their processing stages and the information included in the datasets notwithstanding the manner of their recording and other ways of processing;

10) *an operating process* means a consideration or service process of an authority;

11) *technical interface* means a data transfer solution enabling electronic data transfer between two or more information systems;

12) *a viewing access* means a restricted view implemented for the information system that enables the viewing of datasets;

13) *interoperability of information pools* means the exploitation and exchange of information between different information systems so that the information retains its significance and usability;

14) *machine-readable format* means a file format structured in such a way that software applications can easily identify, recognise and extract datasets, individual data and their structures from it.

Section 3
Scope of application of the Act and restrictions to it

This Act applies to information management and the use of information systems when authorities process datasets unless otherwise provided elsewhere in the law. The provisions of this Act on an authority shall also be applied to universities referred to in the Universities Act (588/2009) and to universities of applied sciences referred to in the Universities of Applied Sciences Act (932/2014).

Separate provisions are issued on the procedures to be complied with in the consideration of matters and service production, secrecy and the right of access to official documents and the archiving of documents. Information management and the use of information systems in the Evangelical Lutheran Church in Finland are governed by the provisions of the Church Act (1054/1993).

Sections 19, 20, 26 and 27 of this Act do not apply to the application of the law by courts of law or committees established to handle appeals. Chapter 3 of this Act does not apply to the activities of the Parliamentary Ombudsman of Finland or the Chancellor of Justice, courts of law or committees established to handle appeals, the Office of the President of the Republic of Finland, Parliamentary organs, Kela, the Bank of Finland, other independent institutions subject to public law, universities referred to in the Universities Act or universities of applied sciences referred to in the Universities of Applied Sciences Act. Chapter 3 of this Act applies to municipalities and joint municipal authorities when performing their statutory tasks.

Chapter 4 and sections 22-27 of this Act apply to private individuals or corporations or corporations subject to public law other than those serving as authorities insofar as they perform public administrative tasks. Private individuals and corporations and corporations subject to public law other than those serving as authorities shall also be governed by the provisions of sections 4 and

28 of this Act when exercising public authority as referred to in section 4, subsection 2 of the Act on the Openness of Government Activities or when said Act has been separately provided to be applied to their activities.

This Act does not apply to the provincial, State and municipal authorities operating in the province of Åland Islands.

Chapter 2
Arrangement of information management

Section 4
Arrangement of information management in information management entities

The information management entities referred to in this Act comprise:

1) State agencies and institutions;

2) courts of law and committees established to handle appeals;

3) Parliamentary organs;

4) State enterprises;

5) municipalities;

6) joint municipal authorities;

7) independent institutions subject to public law;

8) universities referred to in the Universities Act and universities of applied sciences referred to in the Universities of Applied Sciences Act.

The management body of the information management entity shall ensure that the information management entity has:

1) defined the responsibilities connected to the tasks relating to the implementation of information management provided in this Act and in another act;

2) up-to-date instructions for the processing of datasets, the use of information systems, the data processing rights, the implementation of the information management responsibilities and for the rights of access to information, data security measures and preparedness for exceptional circumstances;

3) training available to ensure that the personnel and those acting on behalf of the information management entity have adequate knowledge of the provisions, regulations and instructions of the information management entity in force relating to information management, data processing and publicity and secrecy of documents;

4) proper tools for implementing the obligations relating to information management;

5) organised adequate supervision of compliance with the provisions, regulations and instructions relating to information management.

Section 5
Information management model and assessment of transformative impact

The information management entity shall maintain an information management model which defines and describes the information management in its operating environment. The information management model is maintained to design and implement the management of services, consideration and datasets, to implement the rights and restrictions relating to access to information, to decrease multiple collection of information, to implement the interoperability of information systems and information pools and to maintain information security.

The information management model shall include at least information on:

1) the titles describing the operating processes, the authority responsible for the process, the purpose of the process and the link of the process to other processes;

2) the titles of the information pools, descriptions of the links of the information pools to operating processes and information systems and on the contents of the record referred to in Article 30, paragraph 1 of 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) or, if no record need to be drawn up in accordance with the General Data Protection Regulation, on the authority responsible for the information pool, the purpose of use of the information pool, the central categories of information in the datasets, the information disclosure targets and the storage periods of information;

3) the archiving, manner and place of archiving or destruction of datasets;

4) the titles of the information systems, the authority responsible for the information system, the purpose of use of the information system, the interfaces between the information system and other information systems and the means of data transfer used in the interfaces;

5) data security measures.

When planning essential administrative reforms with an effect on the contents of the information management model and the introduction of information systems, the information management entity shall assess the changes they are subjected to and their impacts in relation to the information management responsibilities, the information security requirements and measures provided in chapter 4, the requirements relating to the production and manner of disclosure of datasets provided in chapter 5, the requirements relating to case management and the information management of services provided in chapter 6 and the publicity, secrecy and protection of documents and the right of access to information provided elsewhere in the law. The information management entity shall, when assessing the changes in information management, take into account the interoperability of the information pools and their exploitation potential when producing and using datasets. On the basis of the assessment, the information management entity shall take the necessary measures to change the information management model and to implement the changes. The data protection impact assessment and the related prior consultation shall be provided for separately.

Chapter 3
General governance of information management in public administration

Section 6
General governance of interoperability of information pools

The general governance of the interoperability of the shared information pools of public administration is the task of the Ministry of Finance. For this purpose, the Ministry of Finance:

1) sees to the maintenance of the information management map of public administration;

2) maintains the general strategies for the development of information management in public administration to promote the interoperability of shared information pools and information systems.

Each ministry shall, within its own mandate, see to the up-to-datedness of the contents of the information management map of public administration and maintain the general strategies to promote the interoperability of shared information pools and information systems. Further provisions on the contents and the implementation of the maintenance of the information management map of public administration may be given by government decree.

Section 7
Cooperation in information management in public administration and the production of information and communication technical services

The Ministry of Finance shall ensure that cooperation practices and procedures for authorities operating in State agencies and institutions and municipal authorities have been arranged for the coordination of the cooperation relating to information management in public administration and the production of information and communication technical services. The purpose of cooperation is to promote the implementation of the objectives of this Act and the development of the public administration practices and the service production methods by utilising information pools and information and communication technology. The development of information management in public administration and information and communication technical services and their changes and impacts are monitored in the cooperation.

The Council of State may appoint advisory committees and other cooperation organs for the cooperation referred to in subsection 1.

Section 8
Assessment of the changes in information management in State agencies and institutions

State agencies and institutions shall assess the financial impacts of changes affecting information management when making the assessment in accordance with section 5, subsection 3.

The ministry in charge of the mandate shall draw up the assessment in accordance with section 5, subsection 3 when the provisions being prepared have an impact on datasets and information systems. The ministry shall also assess the impacts of the planned provisions on the publicity and secrecy of documents.

Section 9
Opinion on the assessment of changes in central government

State agencies and institutions shall submit to the Ministry of Finance the assessment drawn up on the basis of section 5, subsection 3 and section 8, subsection 1 for an opinion on the exploitation potential, interoperability and data security of information pools and information systems when the assessed change has significant financial or operational impacts on information management or operations or when the change involves material changes in the interface data structure of the shared information pools of public administration. The Ministry of Finance shall have the right to obtain, notwithstanding secrecy provisions, the necessary information from a State authority for submitting the opinion.

Further provisions on changes in the information management requiring an opinion, the contents of the request for an opinion and the procedure to be complied with in the opinion matter are given by government decree.

Section 10
Information Management Board of Public Administration

The Information Management Board of Public Administration (the Information Management Board) operates in connection with the Ministry of Finance and its tasks are to:

1) assess the implementation of and compliance with the regulations of section 4, subsection 2; sections 5, 19, 22-24 and 28; and chapter 6 by State agencies and institutions and municipalities and joint municipal authorities;

2) promote the implementation of the procedures of information management and data security provided in this Act and the requirements of this Act.

The Information Management Board is appointed by the Council of State for four years at a time. The Information Management Board has a chairman, a deputy chairman and members who have expertise in data security of public administration, interoperability of information systems and information pools, statistics and information management of datasets. Further provisions on the composition, arrangement of operations, decision-making procedure and qualification requirements of members of the Information Management Board are given by government decree.

The Ministry of Finance assigns part-time secretaries from among its officials to their duties for the term of the board. Further provisions on the tasks of the secretaries are given by government decree.

A member and deputy member of the board shall be governed by the provisions on criminal liability in office when attending to tasks provided for the board. The liability for damages shall be governed by the Tort Liability Act (412/1974). The members and deputy members of the board are paid a fee for attending to the tasks. The Ministry of Finance confirms the amount of the fees.

The Information Management Board may form temporary sections to develop information management procedures. The sections may include experts from the information management entities. The secretaries of the board act as chairmen of the sections. It is the task of the Population Register Centre to produce expert services to the Information Management Board to develop information management and data security procedures.

Section 11
The assessment task of the Information Management Board

The implementation of the assessment task of the Information Management Board is based on an assessment plan approved by the Information Management Board.

To implement the assessment task, the Information Management Board shall have the right to receive from the authorities subject to the assessment, free of charge and notwithstanding secrecy provisions, the reports necessary for attending to the assessment task and the necessary information on the information management model, the assessment of changes in information management, the description referred to in section 28, the procedures used in case management and information management of services, the technology relating to the modification of documents into electronic format, the implementation of viewing access and the description of technical interfaces,

the use and management of technical interfaces and the procedure of use of interfaces with the exception of documents security classified as secret. The authority shall submit the requested information to the Information Management Board by a time limit set.

If the Information Management Board detects failure regarding compliance with the provisions referred to in section 10, subsection 1, paragraph 1 that are being assessed, the Board may call the authority's attention to the implementation of the procedures of and compliance with the requirements relating to information management in accordance with this Act.

The Information Management Board shall draw up a report of the results of the assessment every other year and submit it to the Ministry of Finance.

Chapter 4
Data security

Section 12
Identification of tasks requiring reliability and ensuring reliability

An information management entity shall identify the tasks whose performance requires special reliability from persons employed by it or acting on its behalf. The preconditions for carrying out a security clearance of a person are provided in the Security Clearance Act (726/2014). The right of an employer to acquire personal credit data on an employee in order to establish his or her reliability and to process data on drug use testing are governed by the provisions of the Act on the Protection of Privacy in Working Life (759/2004).

Section 13
Data security of datasets and information systems

An information management entity shall monitor the state of the data security of its operating environment and ensure the data security of its datasets and information systems over their entire lifecycle. The information management entity shall determine the material risks to data processing and dimension the data security measures in accordance with the risk assessment.

The resilience and operational availability of the information systems that are material with regard to performance of the tasks of the authorities shall be ensured with adequate testing on a regular basis.

The authority shall plan the information systems, the internal structure of the information pools and related processing so that the publicity of documents can be easily implemented.

In its acquisitions, the authority shall ensure that appropriate data security measures have been implemented in the information system to be acquired.

Separate provisions are laid down on the assessment of the data security of the information systems and telecommunications arrangements of the authorities.

Section 14
Transfer of data in a data network

An authority shall perform the transfer of data in a public data network using an encrypted data transfer connection or practice if the transferred data are secret. In addition, the data transfer shall be arranged so that the recipient is ascertained or identified in a sufficiently data secure manner before the recipient is allowed to process the transferred secret data.

Identification of the user in digital services provided to the public is governed by the Act on the Provision of Digital Services (306/2019).

Section 15
Ensuring dataset security

An authority shall ensure, with the necessary data security measures, that:

1) the unaltered state of its datasets has been sufficiently ensured;

2) its datasets have been protected against technical and physical damage;

3) the authenticity, timeliness and accuracy of its datasets have been ensured;

4) the availability and usability of its datasets have been ensured;

5) the availability of its datasets is restricted only if access to the information or processing rights have been separately restricted in the law;

6) its datasets can be archived, as required.

The datasets shall be processed and stored in premises which are sufficiently secure with a view to implementing the requirements relating to the reliability, integrity and availability of datasets.

Section 16
Management of access rights to information systems

The authority in charge of the information system shall determine the access rights to the information system. The access rights shall be determined in accordance with the needs relating to the tasks of the user and they shall be kept up-to-date.

Section 17
Compilation of log data

An authority shall ensure that the necessary log data is compiled of the use of its information systems and the disclosure of information therefrom if the use of the information system requires identification or other login. The purpose of use of log data is to monitor the use of the information in the information systems and its disclosure and to investigate technical errors in the information system.

Section 18
Security classified documents in central government

The authorities operating in State agencies and institutions, the courts of law and committees established to handle appeals shall security classify documents and make a security classification marking on them to indicate the information security measures to be complied with when processing the documents. A security classification marking shall be made if the document or the information included therein is secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7-11 of the Act on the Openness of Government Activities and the unauthorised disclosure or unauthorised use of the information contained in the document can cause prejudice to national defence, preparedness for exceptional circumstances, international relations, combating of crime, public safety or the functioning of government finances and the national economy or to the safety of Finland in another comparable manner.

A security classification marking may not be used in cases other than those referred to in subsection 1 unless the making of the marking is necessary to implement an international information security obligation or unless the document is otherwise connected to international cooperation.

Documents referred to in the Act on International Information Security Obligations (588/2004) shall be marked with a security classification as provided in said act.

Further provisions on security classification, the marking to be made in security classified documents and the information security measures relating to the processing of security classified documents are given by government decree. Stamps indicating secrecy to be affixed to documents are governed by the provisions of section 25 of the Act on the Openness of Government Activities.

Chapter 5
Production of datasets and electronic disclosure

Section 19
Modification of datasets into electronic format and access to datasets

If a document is received by an authority in other than electronic format, it shall be modified into electronic format if the document is provided to be permanently preserved or archived by law or under an act. The authority is responsible to ensure that the document modified into electronic format retains its reliability and integrity. Documents prepared by the authority are stored in electronic format. Modification into and storage in electronic format may be derogated from is this is necessary due to the requirements relating to the processing of security classified documents, other information security obligations or another necessary cause relating to the nature of the document.

Having regard to the separate provisions on access to information and the protection of personal data, an authority shall ensure that the dataset is available and exploitable in a commonly used machine-readable format with description data if the dataset can be modified from its original format directly into a machine-readable format.

To modify documents into electronic format, an authority may use a private actor with adequate technical resources and adequate knowledge to attend to such task. The private actor performing this task is governed by the provisions on criminal liability in office. The liability for damages is governed by the Tort Liability Act.

Section 20
Collection of datasets for the tasks of the authorities

An authority shall aim at exploiting the datasets of another authority if the authority is entitled to obtain the necessary information from another authority via a technical interface or a viewing access. When exploiting the information, the legal protection of the party to the matter or another client of the administration shall be ensured.

If an authority is entitled to obtain information from the information pool of another authority for the performance of its tasks in a reliable and timely manner via a technical interface or a viewing access, the authority may not request its client to present or submit such certificate or extract unless this is necessary to clarify the matter.

Section 21
Determining the necessity for storage of datasets

If the storage period of datasets or documents is not governed by law, the following shall be taken into account when determining the storage periods:

1) the necessity of the dataset for the operations of an authority in accordance with its original purpose of use;

2) the implementation and verification of the interests, rights, obligations and legal protection of a natural or legal person;

3) the legal effects of a contract or another legal action governed by private law;

4) statute of limitation in tort law; and

5) statute of limitation in criminal law.

After the end of the storage period, the datasets shall be archived or destroyed without undue delay in a data secure manner.

Separate provisions are issued on the liabilities relating to the determination of storage periods, archiving and the tasks of the archivistics.

Section 22
Disclosure of information between authorities via a technical interface

The authorities shall implement electronic disclosure of information of a regularly repetitive character and standard content between information systems via technical interfaces if the receiving authority has a statutory right of access to the information. Electronic disclosure of information of a regularly repetitive character and standard content may be implemented in another manner if the implementation or use of the technical interface is not technically or financially appropriate. The authority may open the technical interface to an authority with the right of access also in other situations. Separate provisions are laid down on the delivery of documents and information in another manner.

In addition to the provisions of chapter 4, disclosure of information via technical interfaces shall be implemented between information systems so that the case-by-case necessity or essential nature of the information to be disclosed to perform the tasks of the authority receiving information is ensured by technical means if the information to be disclosed is personal data or secret data.

The description of the data structure of the information to be disclosed via a technical interface is determined and maintained by the authority that discloses the information. When planning disclosure of information between several authorities via technical interfaces, the description of the data structure shall be determined and maintained at the direction of the ministry in charge of the mandate.

Section 23
Opening a viewing access for an authority

An authority may open a viewing access for another authority to such information in the information pool to which the authority receiving the viewing access has the right of access. In addition to the provisions of chapter 4, a precondition for opening a viewing access is that:

1) the viewing access is restricted to only individual searches which, in accordance with the right of access, may be directed to necessary or essential information; and

2) the purpose of use of the information is clarified in connection with the search for information.

An authority shall implement the viewing access so that the information system that enables the viewing access automatically recognises irregular searches for information.

Section 24
Disclosure of datasets via a technical interface to other than authorities

An authority may disclose information via technical interfaces to other than another authority if the actor receiving the information has a right of access provided separately in the law and the right to process this information. The technical interface may be opened when the preconditions provided in section 22 are met as provided in said section. The authority disclosing the information shall, where necessary, ensure that the actor receiving the information complies with the obligations provided in this Act for the processing of information.

Separate provisions are issued on the disclosure of information in another electronic format and as information service for the public implemented as a viewing access.

Chapter 6
Case management and information management of services

Section 25
Registration in a case register

An information management entity shall maintain a case register of matters that are being and have been considered by the authorities, into which information on the matter, its consideration and the documents shall be registered. An authority shall, without delay, register a document it has received or drafted in the case register. In addition to the provisions of section 26, the registration of a document shall state the date of arrival of the document.

The information management entity shall ensure that information may be produced of the public entries in the case register or a part thereof to identify requests relating to access to information.

Section 26
Information to be entered in the case register

The information management entity shall form a case identifier specifying a matter admitted or submitted to be considered by an authority with which the information relating to the matter is specified.

The authority shall enter in the register at least the following identification details for the matter:

1) the business ID of the information management entity;

2) identification data of the authority;

3) identification data of the operating process;

4) the date on which the matter became pending.

At least the following are entered in the register of a document received by an authority:

1) document identification data;

2) manner of receipt of the document;

3) the sender of the document or his or her representative.

At least the following are entered in the register of documents prepared by an authority:

1) document identification data;

2) the author of the document;

3) date of preparation.

At least the following are entered in the case register regarding the matter:

1) the party that initiated the matter and, where necessary, other parties to the matter;

2) the consideration stage;

3) the measures by the authority and the documents processed therein per consideration stage.

Section 27

Management of datasets in service production

The information management entity shall arrange the management of datasets generated in connection with other than the consideration of a matter so that the documents composed of the dataset can be searched with an identifier specifying the sets of data so that the information can be easily provided to the party entitled to it. The authority shall, without delay, register the documents and other information generated in service production so that their generation in service production can be verified afterwards.

Section 28

Description to implement document publicity

In order to implement the publicity principle, the information management entity shall maintain a description of the information pools and case register managed by it. The description shall include information on:

1) the information systems containing information belonging to the case register or the information management of services;

2) the authority that decides on the submission of information contained in the case register or the information system and its contact information for requests for access to information;

3) the datasets included in the information systems by data groups;

4) the search parameters with which documents can be technically searched from the case register or information systems of an authority;

5) the open access to datasets via a technical interface.

The information management entity shall publish the description referred to in paragraph 1 in a public data network in so far as the information in the description is not secret.

Chapter 7

Miscellaneous provisions

Section 29
Entry into force

This Act enters into force on 1 January 2020.

This Act repeals the Act on Information Management Governance in Public Administration (634/2011).

Section 30
Transitional provisions

The information management entities shall prepare the information management model in accordance with section 5 within 12 months from the entry into force of this Act.

Authorities other than those operating in State agencies and institutions shall implement the requirements provided in sections 12-16 within 36 months from the entry into force of this Act.

Section 19, subsection 1 of this Act is applied to new documents received or drafted by an authority after 24 months following the entry into force of this Act. Datasets generated prior to the entry into force of the Act are stored as if they had been generated before the termination of the transitional period. Access to datasets referred to in section 19, subsection 2 above shall be implemented within 24 months from the entry into force of this Act. Section 20 of this Act is applied after 12 months following the entry into force of this Act.

The ministries shall, within 12 months from the entry into force of this Act, clarify the information systems referred to in section 22, subsection 3 requiring the management of interface determination and maintenance.

The provisions of sections 17 and 22-24 of this Act apply to information systems acquired after the entry into force of this Act. Information systems acquired prior to the entry into force of this Act are governed by the provisions of sections 22-24 relating to the electronic disclosure of information when the technical interfaces or viewing access of the information systems are up-dated, however, at the latest after 48 months following the entry into force of the Act and the stipulations

of section 17 relating to the requirements to compile log data after 24 months following the entry into force of this Act.

Case management and information management of services shall be arranged within 24 months from the entry into force of this Act in accordance with the requirements provided in sections 26 and 27. The descriptions provided in section 28 of this Act shall be up-dated within 12 months from the entry into force of the Act.