Act

on the Secondary Use of Health and Social Data

By decision of Parliament, the following is enacted:

Chapter 1

General provisions

Section 1

Objective of the Act

The objective of the Act is to enable efficient and secure processing of personal data collected during the provision of social and health care as well as personal data collected for the purpose of steering, supervision, researching and collecting statistics on the social and health care sector. Another objective of the Act is to allow the collected personal data to be combined with the personal data held by Social Insurance Institution of Finland, Population Register Centre, Statistics Finland and Finnish Centre for Pensions.

Furthermore, the Act seeks to secure the legitimate expectations, rights and freedoms of individuals when processing personal data.

Section 2

Scope of application

The provisions of this Act supplement those 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), hereinafter *Data*

Protection Regulation, when the personal data referred to in section 1 are used for the following purposes, even if the data were not originally stored for such a purpose:

1) statistics;

2) scientific research;

3) development and innovation activities;

4) education;

5) knowledge management;

6) steering and supervision of social and health care by authorities; and

7) planning and reporting duty of an authority.

Sections 6 and 7 lay down provisions concerning the organisations whose data may be processed pursuant to subsection 1 of this Act as well as restrictions for the processing.

Chapters 4 and 5 lay down provisions on the grounds for disclosure and the recipient's right to use the disclosed personal data for the purposes referred to in subsection 1.

Section 3

Definitions

In this Act:

1) *customer data* refers to personal data pursuant to Article 4(1) of the Data Protection Regulation that must be kept secret by law and that is stored in a customer register or an associated administrative register as a result of social and health care customership or for processing of benefits;

2) *primary purpose of personal data* refers to the purpose for which the personal data was originally saved;

3) *secondary purpose of personal data* refers to the processing of personal data for a purpose other than the primary purpose referred to in section 2;

4) *development and innovation operations* refers to the application and use of engineering and business data and other existing data together with the personal data referred to in this Act for the purpose of developing new or significantly improved products, processes or services;

5) *knowledge management* refers to the processing of data carried out by a service provider in their customer, service and production processes for the purpose of supporting operations, production, financial control, management and decision-making.

6) *steering of social and health care by authorities* refers to the statutory steering of social and health care organisations by the national social and health care authorities based on personal data and statistics collected for the purpose or on data received for the steering or supervision task on a case-by-case basis.

7) *supervision of social and health care by authorities* refers to the statutory supervision of social and health care professionals and units by the national social and health care authorities;

8) *data permit* refers to a permit pursuant to this Act to process the secret personal data specified in the permit for the purpose specified in the permit;

9) *data request* refers to a request to obtain aggregated statistics created from the personal data referred to in this Act for a purpose compliant with this Act;

10) *secure hosting service* refers to a data secure solution via which the parties can disclose and receive data that is subject to restrictions on access and use;

11) *secure operating environment* refers to a technical, organisational and physical data processing environment in which data security is achieved by appropriate administrative and technical means;

12) *data request management system* refers to a system via which a party applying for a data permit or otherwise requesting data pursuant to this Act submits their data permit application or data request (including any annexes) in accordance with this Act to an authority and in which the applicant is informed of the decision concerning the data permit or data request;

13) *service provider* refers to an authority that organises, produces or implements social and health care or social or health services, or a private service producer referred to in the Act on Private Social Services (922/2011) or Act on Private Health Care (152/1990);

14) *service organiser* a social and health care service provider that:

a) has an obligation as an authority to ensure that the customer gets a service or benefit that according to law or authoritative decision is due to him or her: or

b) has an obligation as a private service provider to ensure that the customer who purchases the service privately is provided with the service that is due to him or her under the regulations on consumer protection;

15) *service producer* refers to a service provider that produces a social or health care service under an agreement made with the service organiser or otherwise on behalf of the service organiser.

16) *service offerer* refers to a party that offers to its clients services associated with a data secure operating environment.

17) *data utilisation plan* refers to a research plan, project plan or a similar plan that states the intended purpose of the data referred to in the permit application, the controller and processors of the data, the legal ground for the processing and the essential factors of the data security and data protection related to the processing throughout the lifecycle of the data, including the storage, erasure or archiving of the data.

18) *aggregated statistics* refers to reliably anonymised data in a statistical format;

19) *pre-processed data* means data from one or more organisations which the data permit authority for the social and health care sector referred to in section 4 has combined into a single whole or stored in a way that has replaced the identifying information in the data with a uniform code;

20) *data security assessment body* refers to a company, community and authority which has been approved by the Finnish Transport and Communications Agency pursuant to the Act on Information Security Inspection Bodies (1405/2011) to assess whether an information system meets the requirements on data security.

Chapter 2

Authorities and organisations

Section 4

Data permit authority for social and health care

The data permit authority (*Data Permit Authority*) referred to in this Act operates within the National Institute for Health and Welfare. The statutory tasks of the Data Permit Authority are carried out by an independent unit at the National Institute for Health and Welfare. The unit is separated from the tasks laid down in section 2 of the Act on the National Institute for Health and Welfare (668/2008).

The Data Permit Authority operates under performance guidance of the Ministry of Social Affairs and Health, has a separate director appointed by the Ministry of Social Affairs and Health and a steering committee also appointed by the Ministry of Social Affairs and Health.

Section 5

Tasks of the Data Permit Authority

The Data Permit Authority makes decisions on data permits concerning data held by other controllers and makes decisions on whether a data request referred to in section 45 conforms to this Act. The Authority is responsible for the collection, combination, pre-processing and disclosure for a secondary purpose of the data associated with its decision in accordance with this Act. Furthermore, the Data Permit Authority may, on the basis of a data request, collect personal data from different controllers for a purpose laid down in this Act and combine such data to generate anonymous data for the requesting party.

The Data Permit Authority maintains a data request management system to forward and process data requests and permit applications. The Authority also maintains a secure hosting service for receiving or disclosing personal data. Furthermore, the Data Permit Authority maintains a secure operating environment in which the permit holder may process the personal data they have been disclosed on the basis of a data permit.

The Data Permit Authority supervises compliance with the terms and conditions of the permit they have issued. The Authority may revoke the data permit if the permit holder fails to comply with the law or the terms and conditions of the permit.

The Data Permit Authority is responsible for anonymising the personal data that serves as the basis of the published results as provided in section 52.

Section 6

Authorities and organisations responsible for the services and restrictions on data sets

Chapter 3 contains provisions on the services that are needed for processing the customer data of social and health care services and other personal data referred to in this Act that can be combined with them for the purposes stated in section 2. The responsibility for producing the services lies with the Data Permit Authority and the following authorities and organisations:

1) Ministry of Social Affairs and Health;

2) National Institute for Health and Welfare, notwithstanding the data it has collected for statistical purposes as a statistical authority.

3) Social Insurance Institution of Finland insofar as the data needed for the purposes stated in this Act is personal data stored during the processing of benefits in a customer relationship or concerns drug prescriptions and associated delivery information stored in a prescription centre referred to in section 3, paragraph 4 of the Act on Electronic Prescriptions (61/2007) and in a prescription archive referred to in paragraph 5 of the Act.

4) National Supervisory Authority for Welfare and Health Valvira;

5) Regional State Administrative Agencies insofar as they process matters related to social and health care;

6) Finnish Institute of Occupational Health insofar as the data needed for the purposes stated in this Act comes from occupational disease registers and exposure measurement registers and the Institute's patient registers;

7) Finnish Medicines Agency Fimea;

8) Public service organisers of social and health care;

9) Statistics Finland insofar as the data needed for the purposes stated in this Act is data referred to in the Act on Determining the Cause of Death (459/1973);

10) Finnish Centre for Pensions insofar as the data needed for the purposes stated in this Act is necessary personal data stored in the Finnish Centre for Pensions's registers and concerns employment and earnings information stored during the implementation of earnings-related pension, granted benefits and their justifications, including disability pension diagnoses; and

11) Population Register Centre insofar as the data needed for the purposes stated in this Act comes from the Population Information System and is basic data on individuals, their family relationships and places of residence as well as data on buildings.

Section 7

Exceptions for the processing of data collected by statistical authorities

As a statistical authority, Statistics Finland and the National Institute for Health and Welfare (*statistical authorities*) are responsible for granting data permits for scientific research that uses the data the authorities have collected for statistical purposes and also for combining the data associated with the research plan to their own data and the pseudonymisation or anonymisation of the data in accordance with the Statistics Act (280/2004). A permit application for other data referred to in this Act as well as data collected by the statistical authorities for statistical purposes shall be submitted to Statistics Finland and the National Institute for Health and Welfare via a data request management system referred to in section 16. Likewise, the system is also used for informing the applicant about the processing of the permit application and the decision on the permit.

The disclosure of data for combination with other data in accordance with the Statistics Act and referred to in this Act is subject to the provisions in Section 51(4).

Section 8

Steering the operations of the Data Permit Authority and developing the co-operation between controllers

To steer the operations of the Data Permit Authority and to develop the cooperation of organisations responsible for services related to the operations, the Ministry of Social Affairs and Health appoints a steering committee for the Data Permit Authority for a three-year period and also appoints a chairperson for the committee. The Ministry of Social Affairs and Health will appoint the following members to the steering committee:

1) Six representatives on the basis of proposals made by the organisations and authorities referred to in section 6;

2) One member to represent municipalities as the organisers of social and health care services;

3) one member on the basis of a proposal by the Association of Finnish Local and Regional Authorities to represent municipalities as organisers of preventive social and health care services;

4) One member to represent the private organisers of social and health care services;

The task of the steering committee is to process and make a proposal to the National Institute for Health and Welfare and the Ministry of Social Affairs and Health on the following:

1) The annual action plan of the Data Permit Authority and the associated budget;

2) Report on operations and financial statements as applicable to the Data Permit Authority;

3) The joint development of controllers and the resources allocated to the task;

4) The resources allocated for each party for the development of information systems and cooperation;

The steering committee monitors the functionality of the operations and services of the Data Permit Authority and the adherence to deadlines on permit processing referred to in section 47 and on data disclosure referred to in section 48. Additionally, the steering committee may:

1) Set goal indicators for the processes of the Data Permit Authority and initiate external audits on the processes;

2) If necessary, make a proposal to the National Institute for Health and Welfare and the Ministry of Social Affairs and Health on the improvement of the Data Permit Authority's operations; and

3) Establish expert groups to support the operations of the Data Permit Authority.

The Ministry of Social Affairs and Health establishes a high-level expert group for the Data Permit Authority. The task of the group is to create guidelines on anonymisation, data protection and data security for the Data Permit Authority's operations. The expert group must have an expert on each of the following fields: artificial intelligence, data analytics, data security, data protection, suitable research, statistics and statistical service as well as a representative of the Data Permit Authority. Further provisions on the tasks of the expert group, the number of its members and their eligibility criteria may be issued by a decree by the Ministry of Social Affairs and Health.

Section 9

Possibility to establish a limited liability company

The Ministry of Social Affairs and Health may establish a limited liability company that operates under the Data Permit Authority. The company can be established by the Ministry of Social Affairs and Health alone or with one or more organisations referred to in section 6, Ministry of Education and Culture, Ministry of Economic Affairs and Employment or the Ministry of Social Affairs and Ministry of Finance. The company will be owned and controlled by the state. The Ministry of Social Affairs and Health will be responsible for the ownership steering and the administration of the shares of the company. The company will be a non-profit company.

The company can be assigned duties related to services referred in section 10, paragraphs 3–7. Further provisions on the duties of the company may be issued by Government decree.

The National Institute for Health and Welfare or the Data Permit Authority may produce administrative services and other support services for the limited liability company for a compensation at a market rate.

If requested by the Ministry of Social Affairs and Health, the company must submit the information needed to steer and supervise the company. The company documents shall be subject to the provisions on official documents in the Act on the Openness of Government Activities (621/1999), hereinafter *Publicity Act*. The decision not to disclose a document to a party requesting it shall be made by the Data Permit Authority in accordance with Chapter 4 of the Publicity Act.

Discretionary government transfers may be granted for the operations of the company from the appropriations in the State budget. The discretionary government transfers are subject to the provisions in the Act on Discretionary Government Transfers (688/2001).

The persons in service of the company and the members company's Board of Directors shall be subject to the provisions on criminal liability for acts in office.

Chapter 3

Services that enable secondary use

Data services

Section 10

Services that organisations provide for secondary use

The following services are maintained by the organisations referred to in section 6 for the secondary use of the data in the registers:

1) Data set descriptions;

2) Advisory service;

3) Collection, combination and pre-processing service for data;

4) Identifier administration service;

5) Data request management system;

6) Secure hosting service;

7) Secure operating environment;

Section 11

Organisations' responsibilities for the services

The Data Permit Authority will always be responsible for the services referred to in section 10, paragraphs 3–7, when the matter concerns a data request referred to in section 45 or when a data permit application concerns the following:

1) Personal data registers of several controllers referred to in section 6;

2) Data stored in national information system services (*Kanta services*) referred to in the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007), hereinafter *Client Data Act; or*

3) Data stored in the registers of one or more private organisers of social or health care services.

However, the only case in which the Data Permit Authority is responsible for the services affecting the data in the registers of the Finnish Centre for Pensions, Population Register Centre and Statistics Finland, is when the data is to be combined with data coming from organisations referred to in section 6, paragraphs 1–8, or with data stored in Kanta services or with data in a registry of a private organiser of social and health care services.

If the data permit application only concerns the data stored in the personal data registers of a single organisation referred to in section 6, paragraphs 1–8, the organisation will be responsible for all services referred to in section 10, paragraphs 1–4. However, the organisations may notify the Data Permit Authority that they will discontinue the maintenance services other than the ones referred to in section 10, paragraphs 1 and 2. In such a case, the Data Permit Authority will assume responsibility for the services related to personal data referred to in section 10, paragraphs 3–7, on behalf of the notifying organisation.

Section 12

Data set descriptions

As controllers, the organisations referred to in section 6 above must create data descriptions of the data content in their data resources in a way that allows the assessment of the suitability of the data for the purposes referred to in section 2. The Data Permit Authority must create data descriptions for their pre-processed data referred to in section 14(5).

The Data Permit Authority issues further orders on the information content, concepts and data structures of the data descriptions. Before issuing the orders, the Data Permit Authority must hear the affected organisations.

Provisions on the starting date of the obligations laid down in subsection 1 shall be laid down by Ministry of Social Affairs and Health decree.

Section 13

Advisory service

The controller referred to in section 6 above must organise the advisory service for the data referred to in section 6 in a way that the party needing the data for purposes stated in section 2 can get sufficient information on the data content of the available registers and the suitability of the data in the registers for their needs.

In addition to the provisions of subsection 1, the Data Permit Authority must organise an advisory service that provides information on the criteria for granting a data permit, the approval criteria for data requests, the content and meaning of services referred to in section 10 and the pre-processed data referred to in section 14(5).

Section 14

Collection, combination and pre-processing service for data

When the Data Permit Authority has granted a data permit referred to in section 44 or has made a favourable decision on a data request referred to in section 45, it collects, combines and pre-processes, and if necessary pseudonymises or anonymises the data for the permit holder or generates the aggregated statistics requested in the data request in accordance with the decision.

If the data permit was granted by a single controller referred to in section 6, paragraphs 1–8 for the data in their own registers, the controller shall generate the data and disclose it to the permit holder for processing in accordance with the permit. However, if the permit requires that the data be disclosed anonymised, the controller must submit the permit and the associated data sets to the Data Permit Authority for combination, pre-processing and anonymisation.

The Data Permit Authority must store a description of the generation of the data sets and aggregated statistics they have disclosed, the pseudonymisation and anonymisation methods they have used and the end results disclosed.

If personal data is disclosed pseudonymised on the basis of several different data utilisation plans, the data must be pseudonymised with a different ID for each disclosure.

The Data Permit Authority may generate pre-processed data sets from the data held by authorities and organisations referred to in section 6. Later, the Data Permit Authority may pick from the pre-processed data set the data needed for granting a data permit, data corresponding to a granted data permit or the data needed for making a decision on a data request.

Section 15

Identifier administration service

The authority that has granted a data permit shall store the identifiers of pseudonymised data sets securely and in a way that allows the replacement of the identifiers in the data set if necessary and the regeneration of the data set.

The authority must store the identifiers as long as necessary to carry out research and verify the validity of its results.

Information systems that serve as a precondition for the operations and ensuring the security of said systems

Section 16

Data request management system

The Data Permit Authority maintains, either alone or jointly with other authorities, a data request management system via which the data permit application or a data request referred to in this Act must be submitted to the authority.

All requests for clarification and supplementary information issued by the Data Permit Authority that serve as a precondition for processing, as well as the clarifications, supplementary information and amendments to the application submitted by the applicant to the authority shall be handled via the management system. The applicant shall be informed of the decision on the permit via the management system.

If the intended purpose requires a statutory ethical preliminary assessment for the data utilisation plan, the ethical assessment will be initiated and the statement delivered via the management system.

Section 17

Secure hosting service

The Data Permit Authority maintains a secure hosting service for the disclosure of data required for the processing of data permit applications and data requests and for the disclosure of data pursuant to a granted data permit. Subject to the conditions laid down in this Act, data may be disclosed via the hosting service between the Data Permit Authority and other authorities referred to in section 6, between the Data Permit Authority and private social and health care service providers and between the permit applicant and the Data Permit Authority.

When personal data is forwarded via the secure hosting service, their integrity and origin must be verified by an electronic signature. The integrity and origin of data transmitted by an organisation and IT devices must be verified by technological means that are as reliable as the electronic signature of a natural person. Strong identification is needed for the users of a secure hosting service when personal data is disclosed to them. Advanced electronic signatures and strong electronic identification are subject to the provisions of the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and the Act on Strong Electronic Identification and Electronic Signatures (617/2009).

The Data Permit Authority must create the necessary interfaces for the interoperability of the hosting service and ensure that data can be transferred by using commonly used technologies.

Section 18

General data security requirements

When personal data is processed pursuant to this Act, the data security level required for processing must be ensured by risk management, access control, active supervision and adherence to the regulations and instructions

issued by the authority responsible for the implementation and supervision of data security and data protection. Special attention should also be given to the implementation of usage restrictions and the confidentiality obligation.

Section 19

Data in logs

When personal data is processed for the permit consideration, decision-making or data disclosure pursuant to this act, the log data must be collected as follows:

1) The Data Permit Authority and the organisation referred to in section 6 must store in usage logs information about the organisation whose data is being used, the user of the data, the data and information groups processed, the intended purpose of the data, the identifier of the data permit application or data request and the time of use of the data; and

2) The Data Permit Authority, a private provider of social and health care services and the organisation referred to in section 6 must store in disclosure logs information about the disclosing organisation, the discloser of the data, the purpose for which the data has been disclosed pursuant to section 2, the identifier of the data permit application or data request, the recipient of the disclosed data and the time of disclosure.

A party processing personal data under a data permit in accordance with this Act must store in their usage logs information about the controller to whom the data permit was granted, the purpose of use pursuant to section 2, the data permit authorising the processing, the user authorised to process the data under the data permit, the data and data groups processed and the time of use.

When a service provider processes personal data residing in their own personal data registers for the purposes of information management, the provider must store in their usage logs information about the personal data used, the user of the data, the purpose of the data and the time of use.

The logs must be erased or archived after 12 years have passed from the expiration of the data permit or the end of processing referred to in subsection 3.

The Data Permit Authority may issue further provisions on the data and content to be stored in the log registers.

Section 20

Secure operating environment

The Data Permit Authority maintains, either alone or jointly with other authorities, a secure operating environment in which the data disclosed by the Data Permit Authority or other authority referred to in this Act can be processed securely and in accordance with the permit.

The processing must be possible by several technical means and the operating environment must be accessible from different locations. The Data Permit Authority must evaluate the level of sensitivity of the data to be disclosed and must take it into account in the requirements it sets for the use of the secure operating environment in the decision on a data permit.

If the data permit application requests that data sets be disclosed for processing in another operating environment than the one referred to in subsection 1, the application must separately state reasons why this is absolutely necessary. In such a case, the Data Permit Authority or another authority referred to in this Act may disclose the data to the applicant only if the operating environment meets the conditions laid down in subsection 2 and sections 21–29.

Section 21

Identifying the users of the secure operating environment

The users of the secure operating environment must be identified reliably and authenticated.

Further provisions on the technical implementation of identification and authentication may be issued by a Ministry of Social Affairs and Health decree.

Section 22

Access rights of the users of the secure operating environment

The service offerer must configure the permit holder's access rights to personal data as well as the access rights of other people who process personal data in the operating environment. The permit holder is granted an access right to the personal data specified in the data permit. Other people who process personal data in the operating environment shall be given access to the essential personal data they need to carry out their tasks.

The service offerer must maintain a register on the users of the secure operating environment and their access rights. The information on the access rights of the users of the operating environment must be erased or archived after 12 years have passed from the expiration of the access right.

The Data Permit Authority shall issue orders on the grounds according to which the service offerer must configure the permit holder's access rights to client data.

Section 23

Protecting the secure operating environment

The secure operating environment must be protected in accordance with the data security obligations of government authorities and in accordance with the provisions of section 36 of the Publicity Act and the Government decree issued pursuant to subsection 1 of the said section.

The operating environment must allow the collection of logs on the use of disclosed data for monitoring and supervision purposes in accordance with section 19.

Section 24

Minimum requirements for secure operating environment

The secure operating environment must fulfil the requirements on data security and interoperability of data transfer that are based on official regulations and recommendations and the standards applicable to a secure operating environment referred to in the regulations and recommendations.

The Data Permit Authority will issue further provisions on the requirements concerning secure operating environments of other service offerers. The requirements must require the same level of data security as is required for the Data Permit Authority's own operating environment.

Section 25

Demonstrating the data security of the secure operating environment

The data security of the operating environment must be demonstrated by a certificate issued by a data security assessment body pursuant to section 26.

The Data Permit Authority may issue further provisions on the procedures to be followed for demonstrating data security.

Section 26

Assessment of data security

Upon an application by the service offerer, the data security assessment body shall assess whether the operating environment meets the requirements on data security in accordance with this Act and the Act on Data Security Assessment Bodies. The assessment must be based on the Data Permit Authority's provisions on the requirements for a secure operating environment.

If the operating environment meets the data security requirements pursuant to this Act, the data security assessment body must issue a certificate on the assessment to the service offerer, including the associated inspection report. If the assessment or reassessment only concerns a part of the operating environment, the certificate issued by the assessment body must clearly state the part of the operating environment that was assessed.

The certificate issued by an assessment body shall be valid for a maximum of five years. The data security assessment body may require the service offerer to provide all data necessary for the assessment, the drawing up of the certificate and the maintenance of the certificate. In all other respects, the issuance of the certificate shall be subject to provisions of section 9(3) of the Act on Data Security Assessment Bodies.

Section 27

Revoking a certificate issued by an assessment body

If a data security assessment body discovers that the operating environment has not fulfilled or no longer fulfills the requirements laid down in this Act or that the certificate should not have been issued for some other reason, the body must request the service offerer to correct the deficiencies. Unless the service offerer corrects the deficiencies by the deadline set by the assessment body, the assessment body may revoke the certificate temporarily or completely or grant it with restrictions. When setting the deadline for corrections, the data security assessment body must take into account the reasonable time it takes to correct the operating environment.

Section 28

Notification obligation of the data security assessment body

The data security assessment body must inform the National Supervisory Authority for Welfare and Health of all granted, changed, supplemented, temporarily revoked, completely revoked or declined certificates and of the requests and restrictions pursuant to section 27. In addition, the data security assessment body must provide any required additional information to the National Supervisory Authority for Welfare and Health upon request.

Section 29

Monitoring of the secure operating environment after deployment

The service offerer must maintain an up-to-date and systematic procedure for monitoring and assessing the experiences of using the secure operating environment when it is in production. The service offerer must monitor the changes to this Act and correct the operating environment accordingly. Any material changes to the operating environment must be reported to the data security assessment body. If material changes are made to the operating environment or if the minimum requirements for the operating environment are changed in ways that necessitate a new assessment, the certificate issued by the assessment body must be renewed.

The service offerer must store the information on conformity to the requirements and other information required by the supervision for at least five years from the date the production use of the secure operating environment ends.

Section 30

Supervision of and audits to information systems

The National Supervisory Authority for Welfare and Health is tasked with the supervision and promotion of the compliance of secure operating environments to the requirements of data security and data protection. The National Supervisory Authority for Welfare and Health maintains a public register on compliant operating environments reported to it.

The National Supervisory Authority for Welfare and Health has the right to carry out audits required for supervision. To perform the audit, the auditor has the right to access all premises that engage in the activities referred to in this Act or store information that is relevant to the monitoring of compliance with this Act. However, the audit may not be carried out in premises intended for permanent residence.

The party being audited must present all documents requested by the auditor that are necessary for carrying out the audit. Moreover, the auditor must be given, free of charge, any copies he or she might request of documents necessary to carry out the audit.

The National Supervisory Authority for Welfare and Health Authority for Welfare and Health must retain the audit report created as a result of the audit for ten years after the audit has been completed.

Section 31

The right of the National Supervisory Authority for Welfare and Health to use external experts

The National Supervisory Authority for Welfare and Health has the right to use external experts to assess the conformity of a secure operating environment. The external experts can participate in the audits referred to in this Act and inspect and test operating environments. The external expert must have the competence and qualifications required to carry out his or her tasks.

When carrying out the tasks referred to in this Act, the external expert is subject to the provisions on the disqualification of public officials laid down in the Administrative Procedure Act (434/2003) and criminal liability for acts in office.

Section 32

Right to information of the National Supervisory Authority for Welfare and Health

The National Supervisory Authority for Welfare and Health has the right to obtain, free of charge and notwithstanding the provisions on secrecy, the information necessary for the supervision of operating environments from the government and municipal authorities as well as the natural persons and legal persons to whom the provisions of this Act or provisions issued by virtue of this Act apply.

Section 33

Regulation issued by the National Supervisory Authority for Welfare and Health to correct defects and a penalty payment

Based on an audit carried out pursuant to section 30, the National Supervisory Authority for Welfare and Health may order a service offerer to correct defects in an operating environment in production use.

If a secure operating environment might jeopardise data protection or if it fails to implement the requirements laid down in this Act and the defects have not been corrected by the deadline set by the National Supervisory Authority for Welfare and Health, the National Supervisory Authority for Welfare and Health can prohibit the use of the operating environment until the defects have been corrected. Furthermore, the Data Permit Authority or other authority referred to in section 6 can prevent access to the information systems maintained by them, if a party using the systems or an external system connected to the systems might jeopardise their proper operation.

The National Supervisory Authority for Welfare and Health may obligate the service offerer or an authorised representative to issue a notification on the decision concerning the production use of the operating environment by the deadline and manner set by the National Supervisory Authority for Welfare and Health.

To enhance a decision it has made pursuant to subsection 1, the National Supervisory Authority for Welfare and Health may issue a notice of a conditional fine or a threat that the operations be terminated partially or completely or that an unperformed action will be performed at the other party's cost. The National Supervisory Authority for Welfare and Health must communicate its decision to the Data Permit Authority.

Section 34

Regulation to fulfill duties

If a service offerer, an authority referred to in section 6 or a party otherwise processing personal data in accordance with this Act has neglected its obligations concerning information systems or their use laid down in this Act, the National Supervisory Authority for Welfare and Health may order the obligation to be fulfilled by a given deadline.

In addition, the Data Permit Authority or other authority referred to in section 6 may prevent access to the information systems it maintains, if a service offerer, an authority referred to in section 6 or a party otherwise processing personal data in accordance with this Act continues to neglect its obligations concerning information systems or their use laid down in this Act even after the deadline set by the National Supervisory Authority for Welfare and Health.

To enhance a regulation it has made pursuant to subsection 1, the National Supervisory Authority for Welfare and Health may issue a notice of a conditional fine or a threat that the operations be terminated partially or completely or that an unperformed action will be performed at the other party's cost. The National Supervisory Authority for Welfare and Health must communicate its decision to the Data Permit Authority.

Chapter 4

Justifications and preconditions to the secondary use of personal information

General justifications for secondary use

Section 35

Justifications for the processing of personal data

The data in the registers of controllers referred to in section 6 above or in the registers of a private organiser of social and health care may be processed for secondary use under a temporary data permit issued by the controller or the Data Permit Authority or directly based on provisions of law as laid down below.

Section 36

The Data Permit Authority's right to obtain and process data without prejudice to secrecy obligations

Secrecy obligations and other restrictions on the use of data notwithstanding, when the Data Permit Authority needs the following data to carry out its tasks laid down in this Act, it has the right to obtain the data from the controllers referred to in section 6, private providers of social and health care services and the Social Insurance Institution of Finland when the data is stored in the Kanta services referred to in the Client Data Act:

1) The information needed to grant a data permit;

2) The data referred to in a granted data permit in order to collect, combine and pre-process the data in accordance with section 14 and to disclose the data for processing by the permit holder;

3) The information needed to assess whether the data referred to in the data permit application can be anonymised or whether aggregated statistics can be produced from data referred to in section 45.

4) The data needed to generate aggregated statistics; and

5) The data needed to collect the pre-processed data sets referred to in section 14(5).

The data referred to in subsection 1 above may be disclosed to the Data Permit Authority via a secure hosting service referred to in section 17.

Secrecy obligations and other restrictions on the use of data notwithstanding, the Data Permit Authority may use a secure hosting service referred to in section 17 to pick the data referred to in the data permit from data and data repositories of controllers referred to in subsection 1 when possible and appropriate in light of the content and technical implementation of the registers and data repositories.

The Data Permit Authority is considered a controller for the data it obtains by the means referred to in this section.

Using data as aggregated statistics

Section 37

Development and innovation activities

Secrecy obligations notwithstanding, the Data Permit Authority may, in individual cases, generate aggregated statistics based on a data request referred to in section 3 paragraph 9 from client data and other personal data

possessed by organisations referred to in section 6, when the aggregated statistics are produced for development and innovation activities other than scientific research referred to in section 38.

The data referred to above in subsection 1 may be disclosed pursuant to section 45 on the condition that the data request and the data utilisation plan attached to it states that the purpose of the activity is to:

1) promote public health or social security; or

2) develop the social and health care services or the service system; or

3) protect the health or wellbeing of individuals or secure their rights and liberties associated with health or wellbeing.

Data disclosed under a data permit

Section 38

Data permit for scientific research and statistics

Secrecy obligations notwithstanding, a data permit may be granted in individual cases to client data and other personal data held by organisations referred to in section 6.

The freedom of scientific research must be ensured when procuring a data permit.

Further provisions on the processing of data for scientific research and statistics are laid down in the Data Protection Act (1050/2018).

Section 39

Education

The client data of a social or health care service provider may be processed without prejudice to secrecy obligations and pursuant to the Article 9 (2g) of the Data Protection Regulation in order to produce educational materials for people processing client data in social and health care and for people studying to become professionals in social and health care, if the materials are necessary to fulfill the goals of the education. A further condition to processing is a granted data permit referred to in this Act.

Furthermore, data containing identifiers may be used for education only when the education cannot be carried out using anonymous data due to the rarity of the case being taught, the nature of teaching or other such reason. The person providing the education must inform the people undertaking the education of the statutory secrecy obligation and the sanctions for breaching it.

A data subject does not have the right, pursuant to Article 21 of the Data Protection Regulation, to object to the processing of his or her personal data for educational purposes, if the processing of personal data is necessary due to the rarity of the case.

The permit holder must erase the separate data sets collected for educational purposes when the data sets are no longer needed for their intended purpose.

Section 40

Planning and reporting duty of an authority

Client data necessary for the planning and reporting duty of an authority as well as other personal data of organisations referred to in section 6 may be processed pursuant to Article 9 (2g) of the Data Protection Regulation provided that the following conditions are met:

1) a data permit referred to in this Act is granted for the processing.

2) the processing is based on an appropriate data utilisation plan; and

3) the planning and reporting duty or the need for data associated with it cannot be fulfilled without processing personal data.

Processing data under law but without a data permit

Section 41

Knowledge management

A social or health care service provider has the right, without prejudice to secrecy obligations and pursuant to Article 9 (2h) of the General Data Protection Regulation, to process and combine identifiable customer data that has been generated in the operations of the provider or stored in the provider's registers, if absolutely necessary to produce, monitor, evaluate, plan, develop, manage and supervise the services the service provider is responsible for.

If the service provider needs to compare their operations to the operations of other service providers in order to evaluate, plan or develop the services or service chains they are responsible for, the Data Permit Authority may generate the data sets required for comparison as aggregated statistical data pursuant to section 45 on the basis of a data request referred to in section 3, paragraph 9.

In addition to the provisions in subsection 1 and 2, a municipality or a joint municipal authority has the right to process and combine identifiable client data stored in a joint register referred to in section 9(1) of the Health care Act (1326/2010), when the purpose of such processing and combination is knowledge management.

Section 42

Steering and supervision of social and health care by authorities

If, in order to carry out its statutory steering and supervision duty, a steering or supervisory authority for social and health care needs combined data that is based on personal data in social and health care registers or identifiable data in registers of other controllers referred to in section 6, the Data Permit Authority may generate the required aggregated statistics pursuant to section 45, based on a data request referred to in section 3, paragraph 9.

Data referred to in subsection 1 that the supervisory authority referred to in the same subsection is entitled to obtain by law without prejudice to secrecy obligations may also be disclosed in identifiable form upon a justified request.

The data referred to in subsection 2 above may be disclosed to the supervisory authority via a secure hosting service referred to in section 17.

Chapter 5

Processing of a data permit application, a data request and the data to be disclosed

Section 43

General grounds for granting a data permit

A data permit to personal data may be granted, if the intended purpose of the data stated in the application and data utilisation plan conforms to the provisions of the Data Protection Regulations, Data Protection Act, this Act and any act applicable to the data and if the most appropriate way to implement the intended purpose is to use the data referred to in the application.

If the data permit application is associated with an intended purpose for which separate provisions have been laid down concerning the application procedure and the grounds for granting the permit, all grounds for granting the permit must be met.

If the data to be disclosed have been collected on the data subject's consent, a data permit for data concerning the data subject may be granted only if it conforms to the terms and conditions of the consent and the disclosure and use of the data. If the intended purpose of the data applied for in a data permit application is based on a data subject's consent, the data permit may only be granted to data that is covered by the data subject's consent.

A data permit can be given for a fixed period if it is obvious that the disclosure of the data does not infringe on the interests safeguarded by the secrecy obligation. The permit must contain appendices that state the requirements for

the security measures for data processing in proportion to the risks involved and other provisions necessary for protecting private interests. A data permit may be revoked if sufficient reasons are considered to exist.

If the Data Permit Authority states concerning a data permit application that instead of a data permit, the matter can be processed as a data request pursuant to section 45, the Data Permit Authority must contact the applicant and propose that the matter be processed as a data request. If the applicant demands that the data permit application be processed, the Data Permit Authority must make a decision on the matter.

Section 44

Competence associated with the processing of a data permit

The Data Permit Authority is always responsible for making a decision on a data permit when the data permit application concerns the following:

1) Data of several controllers referred to in section 6, paragraph 1–8.

2) Data stored in the Kanta services; or

3) Data stored in the registers of one or more private organisers of social or health care services.

In addition, the Data Permit Authority is responsible for making decisions on data permits that concern the data of the Finnish Centre for Pensions, Population Register Centre and Statistics Finland referred to in section 6, paragraph 9–11, if the data is to be combined with data referred to in subsection 1, paragraph 1-3.

If the data permit application only concerns the data stored in the personal data registers of a single organisation referred to in section 6, paragraphs 1–8, the organisation will be responsible for making the decision on the data permit. However, if the organisation has notified the Data Permit Authority pursuant to section 11(3) that they will discontinue the maintenance of services other than those referred to in section 10, paragraph 1 and 2, the Data Permit Authority will be responsible for making decisions on data permits that concern personal data referred to in this Act held by the organisation.

The authority responsible for a decision on a data permit has the right to request a statement on the data permit application from the Data Protection Ombudsman, if the authority considers it necessary.

Section 45

Processing of a data request

A Data Permit Authority makes a decision on whether a data request referred to in section 3, paragraph 9, is compliant with the intended purposes laid down in section 2(1) and other requirements set for a data request.

When making the decision, a Data Permit Authority must assess whether it is possible to generate the aggregated statistics referred to in the data request from the data in the registers stated by the requestor. This assessment must be based on Article 9 (2g) and Article 86 of the Data Protection Regulation and must take into account the guidelines of the expert group referred to in section 8(4).

However, if the purpose of the data request is scientific research and also applies to data collected by a statistical authority for statistical purposes, the procedure must follow the provisions laid down in section 7 and section 51(4).

Section 46

Submitting a data permit application and a data request to the Data Permit Authority

A data request and a data permit application must be submitted to the Data Permit Authority via a data request management system referred to in section 16. If the applicant supplements their application, the supplement must also be submitted to the Data Permit Authority via the data request management system. A data utilisation plan must be attached to the permit application and data request on aggregated statistics.

The Data Permit Authority issues provisions on the data content and data structures of the data permit application, data utilisation plan and the data request.

Section 47

Deadlines for the processing of a data permit

The decision concerning a data permit application must be given without delay, however not later than three months after authority has received the complete application.

If compelling reasons exist, the Data Permit Authority may decide that the processing time of a data permit application be extended for a maximum of 3 months, if the processing of the application and the associated data utilisation plan require unusually extensive processing of data from several different controllers or a particularly challenging consideration process. The Data Permit Authority must inform the permit applicant of the extension of the deadline, the justification for the extension and the new deadline by which the decision on the permit is issued.

If the authority responsible for the decision concerning a data permit requests a statement referred to in section 44(4) from the Data Protection Ombudsman, the processing deadline of the authority responsible for the decision on the data permit will be suspended until the statement arrives.

The controller referred to in section 6 above and a private provider of social or health care services must, upon request and without delay, disclose to the Data Permit Authority the data required for the processing of a data permit application or a data request for aggregated statistics referred to in section 45, in any case no later than 15 working days from the reception of the request.

Section 48

Deadlines for data disclosure

The controller referred to in section 6 above and a private provider of social or health care services must, upon request by the Data Permit Authority and without delay, disclose the data referred to in a granted data permit or the data required to process a data request for aggregated statistics referred to in section 45, in any case no later than 30 working days from the date the Data Permit Authority made a favourable decision on disclosing the data to the applicant. If the report presented by the applicant in support of the data disclosure is insufficient, the Data Permit Authority must inform the applicant without delay of the required additional clarifications. In such a case, the requested data must be submitted to the applicant within 30 working days from the reception of the additional clarification, if the submitted additional clarification enables the Data Permit Authority to verify that the requirements for data disclosure are met.

If the disclosure of data to the Data Permit Authority is not possible within the deadline referred to in subsection 1, the controller must report the delay, its cause and the deadline extension required for data disclosure before the deadline is reached. The Data Permit Authority must set a new deadline for the data disclosure for a justified reason.

The data collected and combined by a Data Permit Authority pursuant to a data permit application must be disclosed to the permit holder without delay, in any case no later than 60 working days from the granting of the permit.

If compelling reasons exist, the Data Permit Authority may extend the deadline for the disclosure of the data if the intended use of the data requires unusually extensive processing of data from several different controllers or a particularly challenging combination process. The Data Permit Authority must inform the permit holder of the extension of the deadline, the justification for the extension and the new deadline by which the data will be disclosed.

Section 49

Fees charged for a data permit and a decision on a data request

The Data Permit Authority or other authority that has granted the permit may charge a fee for the data permit and the decision on a data request. The grounds for the fee are laid down in the Act on Criteria for Charges Payable to the State (150/1992).

Section 50

Fees charged for services

A Data Permit Authority may charge a fee for the picking, delivery, combination, pre-processing, pseudonymisation and anonymisation of data pursuant to a data permit referred to in this Act as well as for the use of a secure operating environment.

The compensation for picking and delivering data in accordance with the data permit from other data repositories than those of the Data Permit Authority is determined by virtue of regulations that apply to the controllers who deliver the data. A controller or a personal data processor who discloses data to the Data Permit Authority by virtue of a data permit referred to in this Act is entitled to such a compensation, which is paid by the Data Permit Authority and is an appropriate proportion of the cost compensation the permit holder is ordered to pay.

Upon request, a party entitled to a compensation under this section must deliver to the Data Permit Authority an estimate of costs that the processing of data causes to the party entitled to a compensation. Based on the information received, the Data Permit Authority will create a cost estimate for carrying out the data request and will deliver the cost estimate to the permit applicant. The Data Permit Authority will charge the permit holder the compensations referred to in subsection 2 and will pay them to the controllers who provided the data.

The grounds for the fees to be paid to the Data Permit Authority are laid down in the Act on Criteria for Charges Payable to the State. Provisions on the fees charged for an assessment by a data security assessment body are laid down in section 11 of the Act on Data Security Assessment Bodies.

The registration and entry into a public register of a notification to the National Supervisory Authority for Welfare and Health pursuant to section 30(1) is subject to a fee.

Section 51

Processing and disclosure of data sets to the permit holder after the data permit has been granted

If the Data Permit Authority has granted a data permit in the circumstances required in section 44, it collects and, if necessary, combines and pre-processes as well as pseudonymises or anonymises the data specified in the data permit and discloses the resulting data sets to the permit holder for processing pursuant to subsection 3 of this section.

If a single controller referred to in section 44(3) has made a decision on a data permit concerning the data in its own registers, it collects the data from the registers and, if necessary, combines, pre-processes and pseudonymises them and then discloses the data sets to the permit holder for processing pursuant to subsection 3 of this section. However, if the data sets are to be disclosed to the permit holder anonymised, the controller must submit the decision on the permit and the data pursuant to the permit to the Data Permit Authority for combination, pre-processing and anonymisation. The Data Permit Authority is always responsible for anonymising the data to be disclosed and disclosing them to the permit holder for processing.

The data sets based on the data permit are always disclosed to the permit holder via a secure hosting service referred to in section 17 for processing in a secure operating environment referred to in section 20, unless aggregated statistics have been created from the data. The data sets referred to in subsection 1 and 2 of this section are primarily disclosed for processing in a secure operating environment referred to in section 20(1) which is maintained by the Data Permit Authority. However, the data sets may be disclosed to be processed in another secure operating environment than the one referred to in section 20(3), if the data utilisation plan and the data permit state a separate reason that necessitates it.

If the intended purpose also required data collected by Statistics Finland or the National Institute for Health and Welfare as a statistical authority for statistics purposes, the statistical authority will combine and, if necessary, pre-process and pseudonymise or anonymise the data to be disclosed. If the intended purpose requires data from both statistical authorities, the authorities together agree which one of them will combine and pseudonymise or anonymise the data. Subsequently, the data may be disclosed via the secure hosting service referred to in section 17 for processing by the recipient either in a secure operating environment maintained by Statistics Finland or the Data Permit Authority or in another operating environment referred to in section 20, depending on the nature and quantity of the data.

Before opening the connection to the permit holder, the service offerer of the operating environment must verify that the permit holder fulfils the requirements stated in the data permit.

Section 52

Publishing results derived from data disclosed by virtue of a data permit

When data has been disclosed for processing in a secure operating environment referred to in section 20 and the results generated are to be published, the Data Permit Authority is responsible for verifying that the data to be published is anonymised. However, the Data Permit Authority may, for a justified reason, issue a permit decision that grants the permit holder the right to carry out the anonymisation of the data to be published by themselves on the condition that the data be delivered later to the Data Permit Authority.

The Data Permit Authority generates the anonymised results and discloses them to the permit holder to be published freely on the basis of the permit holder's request and the proposal attached to the request regardless of whether the data permit was granted by an individual controller or a Data Permit Authority.

Section 53

Reporting obligation of the authorities responsible for processing data permits

The authorities responsible for the processing of data permits must submit at least once a year a detailed report to the Data Protection Ombudsman on the processing of data and log register data they have performed pursuant to this Act.

Section 54

Secrecy obligations

If the data obtained by virtue of this law does not originate from an authority, it is nevertheless also subject to the following sections of the Publicity Act:

1) Section 22 on document secrecy;

2) Section 23 on the secrecy obligation and prohibition of use;

3) Section 24 on secret information;

4) Section 31 on the declassification of a document;

5) Section 32 on the application to the duty of non-disclosure;

If secret data is disclosed by virtue of this Act to a party other than an authority, the recipient of the data must be informed of the secrecy obligations during the disclosure in accordance with Section 25 of the Publicity Act.

Notwithstanding provisions elsewhere in the law on the right or obligation to disclose secret information, the data collected by virtue of this Act may not be disclosed for purposes of administrative decision-making that concerns a private person nor any other processing of matters without the person's explicit consent. However, a supervisory authority for social and health care may use the data it has received pursuant to section 42 for supervisory duties

associated with a person other than the data subject when assessing the lawfulness or professional appropriateness of the operations of health care units and health care professionals.

Chapter 6

Miscellaneous provisions

Section 55

Rights, obligations and actions based on significant clinical findings

Notwithstanding the provisions of section 54(3), a data permit holder has the right to notify the person in charge appointed by the Data Permit Authority of a clinically significant finding that would enable the prevention of a risk to a certain patient's health or significant improvements to the quality of care.

If the notification referred to in subsection 1 is based on anonymous data, the person in charge must determine the person or persons to whom the data applies. When the Data Permit Authority's person in charge knows the persons or persons to whom the notification referred to in subsection 1 applies, the person in charge must submit the information without undue delay to the expert appointed by the National Institute for Health and Welfare.

The expert referred to in subsection 2 above must, in collaboration with other experts appointed by the Institute, assess the significance of the information and the expected benefits of actions that can be taken as a result of the information. If the benefit is estimated to be so obvious that the person should be brought in contact with health care, the expert of the National Institute for Health and Welfare referred to in subsection 2 must report the finding to the unit that is regionally responsible for providing health care to the person pursuant to the Health Care Act.

The unit referred to in subsection 3 above must contact the patient and find out whether he/she wants to be informed of a clinically significant finding and the potential examinations and treatment operations carried out as a result, including the benefits of such examinations and treatment.

The patient has the right to prohibit contacts made due to a clinically significant finding. The prohibition is recorded to the patient's information management system referred to in section 14 of the Client Data Act. The patient may set the prohibition in writing on any unit that produces public health care or electronically via the citizen's user interface referred to in section 19 of the Client Data Act.

Section 56

Steering, supervision and monitoring

The general steering, supervision and monitoring of the processing of personal data pursuant to this Act and of the associated information management is the task of the Ministry of Social Affairs and Health.

The Data Protection Ombudsman, the National Supervisory Authority for Welfare and Health and the Data Permit Authority steer and supervise compliance with this Act within their area of operation and in accordance with the competence provided for them.

The Data Permit Authority and other authorities granting data permits pursuant to this act as well as the National Supervisory Authority for Welfare and Health must monitor and supervise that data protection and data security is realised in their respective services and that the terms and conditions of the permits they grant are followed. If a party has processed personal data illegally, the appropriate authority must start the required actions at their own initiative. If data is processed pursuant to section 20(3) in another environment than the secure operating environment of the Data Permit Authority, the log data referred to in section 19 and the data in a user register referred to in section 22(2) must be delivered to the Data Permit Authority upon request and without undue delay in order to implement the monitoring and supervision.

If the Data Permit Authority or an authority granting data permits by virtue of this Act has a justified reason to suspect that the party processing data under a data permit granted by the authority does not process personal data in compliance with the law, the authority must notify the Data Protection Ombudsman without delay.

Section 57

Obligation of the Data Permit Authority to report to the steering committee

The Data Permit Authority must report to the steering committee all cases in which the deadlines laid down in section 47 and 48 are deviated from and must publish information about the cases.

Section 58

Appeal

A claim for rectification of a decision may be made as laid down in the Administrative Procedure Act to the authority that made the decision, when the decision concerns a data request referred to in section 45 of this Act or when the decision is made by the Data Permit Authority or a controller referred to in section 6 and concerns a data permit

application and the revocation of a data permit, as well as when the decision is one made by the National Supervisory Authority for Welfare and Health by virtue of this Act.

An appeal against a decision issued following a claim for rectification may be made to an administrative court as laid down in the Administrative Judicial Procedure Act (586/1996). An appeal may be made against the decision of an administrative court only if the Supreme Administrative Court grants leave to appeal.

Section 59

Entry into force

This Act enters into force on 1 May 2019.

Section 60

Transitional provisions

Section 19 on log data, section 20(3) and sections 21–34 on the requirements for a secure operating environment and section 55 on clinical findings will apply from 1 May 2021. Before that date, data may be disclosed to a permit holder for processing under section 51(1 and 2), even if the data permit application does not appoint a secure operating environment referred to in section 51(3) for the processing of data.

The deadlines for data disclosure laid down in section 47(4) and section 48 above will apply to the Social Insurance Institution of Finland and the organisers of social care services from 1 January 2024 onwards; to the prescription centre referred to in section 3, paragraph 4 of the Act on Electronic Prescriptions and to the data on drug prescriptions and associated delivery information stored in a prescription archive referred to in section 3, paragraph 5 of the same Act the deadlines will apply from 1 January 2021 onwards.

This Act will apply to the Kanta services referred to in the Client Data Act from 1 January 2021 onwards.

Before the Act enters into force, the data collected with the consent of the data subject may be used and disclosed under this Act for purposes laid down in section 2(1), paragraph 1, 2 and 7, without prejudice to the provisions in section 43(3) if it is obvious that such use and disclosure of the data does not differ from the purposes for which the data has been given. The authority that makes a decision on a data permit may require that the applicant request an ethical assessment from the ethical board of the National Institute for Health and Welfare as grounds for the permit decision.

The processing of an application submitted before this Act entered into force will be completed by applying the provisions that were in force when this act entered into force. However, an application for the disclosure of personal

data in accordance with section 4 of the Act on National Personal Data Files in Healthcare (556/1989) will not be subject to the obligation laid down in subsection 1 of the aforementioned section by which the Data Protection Ombudsman is reserved the right to be heard. Instead, the right to request a statement from the Data Protection Ombudsman on the data permit application pursuant to section 44(4) of this Act will apply.

Section 13 of this Act on an advisory service will apply from 1 November 2019.

Section 41(2), 42(1) and 45 of this Act that apply to the processing of a data request on aggregated statistics will apply from 1 January 2020 onwards.

Section 14(1 and 2) on a data collecting, combination and pre-processing service, pseudonymisation and anonymisation, section 16 on the data request management system and section 20(1) of this Act on a secure operating environment will apply from 1 January 2020 onwards.

Competence associated with the processing of a data permit will be determined under section 44(1–3) of this Act from 1 April 2020 onwards. A data request and a data permit application must be submitted to the Data Permit Authority via a data request management system referred to in section 16 from 1 April 2020 onwards.

Helsinki, 26 April 2019

President of the Republic of Finland

Sauli Niinistö

Minister of Family Affairs and Social Services

Annika Saarikko