Finnish Social and Health Data Permit Authority Date 19 Jan 2022

Date of issue of the regulation	19/01/2022
Effective date of the regulation	19/01/2022
In effect	Until further notice
Standard to be repealed	Regulation by the Health and Social Data Permit Authority 1/2020
Legal basis	Act on the Secondary Use of Health and Social Data (552/2019), section 22(3) and section 24(2) (in the regulation referred to as the “Act on Secondary Use”)

Regulation by the Health and Social Data Permit Authority: Requirements for other service providers' secure operating environments

1 Background

The Health and Social Data Permit Authority Findata (hereinafter “data permit authority”) maintains a secure operating environment in accordance with section 20(1) of the Act on Secondary Use. The data sets for which the data permit authority has granted a permit for use are, as a rule, disclosed for processing by the permit holder in the operating environment in question.

If the data permit application requests that data sets be disclosed for processing in another operating environment than the data permit authority’s secure operating environment, the application must, according to section 20(3) of the Act on Secondary Use, separately state reasons why this is absolutely necessary. In such a case, the data permit authority or another authority referred to in this Act on Secondary Use may disclose the data to the applicant only if the operating environment meets the conditions laid down in section 20(2) and sections 21–29.

If an individual controller referred to in section 44(3) of the Act on Secondary Use has made a decision on a data permit concerning data included in its own registers, it must always disclose the data sets for processing by the permit holder in the secure operating environment referred to in section 20 of the Act on Secondary Use.

According to section 24(2) of the Act on Secondary Use, the data permit authority will issue further provisions on the requirements concerning secure operating environments of other service providers. The requirements must require the same level of data security as is required for the data permit authority's own operating environment.

Before the regulation entered into effect, a round for comments was organised from 26.11.2021 to 17.12.2021, during which a total of 23 comments were submitted. These comments were taken into account in the preparation of the regulation.

The requirements for a secure operating environment are included as Annex 1 to this regulation.

2 Scope of the regulation

This regulation is the data permit authority's provision on the requirements concerning secure operating environments of other service providers, referred to in section 24(2) of the Act on Secondary Use.

This regulation replaces regulation THL/2492/4.00.00/2020, which entered into force on 5 October 2020.

This provision applies to all purposes laid down in the Act on Secondary Use for which a data permit is required under the Act on Secondary Use. These purposes include scientific research, statistics, teaching and the planning and investigation tasks of the authorities. With regard to teaching, the regulation pertains to the preparation of teaching materials, not actual teaching.

Implementation of the requirements laid down in this regulation is a prerequisite for the data permit authority to consider and disclose data sets for processing by the permit holder in an operating environment other than its own in accordance with 20(3) of the Act on Secondary Use. The regulation shall apply from 1 May 2022 at the latest in accordance with the new transitional provision (section 60(1) of the Act amending the Act on Secondary Use of Health and Social Data, 793/2021), which entered into force on 1 September 2021.

3. Grounds for issuing a certificate

Compliance with the requirements of this regulation is proved by a certificate issued by a data security assessment body in accordance with section 26 of the Act on Secondary Use. The certificate is issued on the basis of the findings of the inspection report. In order for the certificate to be issued, the inspection report must meet all of the following conditions:

- The inspection report must not contain any findings classified as serious deviations under this regulation.
- If the inspection report identifies one or more findings classified as an intermediate deviation under this regulation, the inspection report must also include a corrective action plan approved by the assessment body, which also provides for a time limit for the completion of the reassessment. The reassessment shall be carried out successfully no later than 6 months after the completion of the inspection report.
- The combination of non-serious deviations is estimated not to constitute a serious deviation.

The assessment of the data security of the secure operating environment and the accountability for data security using a certificate are provided for in sections 25–29 of the Act on Secondary Use.

4 Validity of the regulation and amendments

This regulation replaces previous regulation THL/2492/4.00.00/2020 of 5 October 2020. That previous regulation shall expire on the entry into force of this regulation. This regulation shall be valid until further notice and contain more detailed and specific provisions than those in the previous regulation on the requirements set for secure operating environments of other service providers.

5 Applicable legislation

The Act on Secondary Use of Social and Health Data (552/2019), sections 18–34, section 60(1), and the Act amending the Act on Secondary Use of Social and Health Data (793/2021), section 60.

Johanna Seppänen
Director

Heikki Lanu
Head of ICT

This regulation has been signed electronically.