Supervision of Region Southern Denmark's use of personal data for research

Date: 20-07-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Data processor

Sensitive information

The Norwegian Data Protection Authority selected three research projects as the subject of the inspection within the subjects "processing basis" and "responsibilities and roles". The Danish Data Protection Authority did not find occasion to express criticism of the region's assessment of the processing basis in the projects, but instead expressed criticism of two of the region's data processing agreements.

Journal number: 2020-422-0026

Summary

The Danish Data Protection Authority has completed a written inspection of Region Southern Denmark with a focus on the processing of personal data in the research area.

As part of the inspection, the Danish Data Protection Authority received, among other things, a list of ongoing research projects at Region Southern Denmark, a more general list of processing activities in the research area in the region as well as the region's guideline for data processing agreements and supervision of data processors. The Norwegian Data Protection Authority selected three research projects as the subject of the inspection within the subjects "processing basis" and "responsibilities and roles".

The Danish Data Protection Authority found no reason to override Region Southern Denmark's assessment of the basis for the processing of personal data in the three projects.

However, the Danish Data Protection Authority expressed criticism that, as far as two data processing agreements were concerned, the region had not demonstrated that they had decided on the level at which the region, as data controller, would supervise their data processors. In this connection, the region had also not demonstrated that their guideline for supervision of

data processors had been followed.

Decision

The Danish Data Protection Authority hereby returns to the case, where on 9 October 2020 the Danish Data Protection Authority launched a written inspection of Region Southern Denmark with a focus on the region's processing of personal data for research use.

The Norwegian Data Protection Authority subsequently selected three research projects within the subjects of "processing basis" and "responsibilities and roles", to which the decision below relates.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that the processing of personal data in connection with the research projects could take place within the framework of the rules in the data protection regulation[1].

The Danish Data Protection Authority, however, finds reason to criticize the fact that, with regard to the data processor agreement for research project no. 1 and the data processor agreement with one of the data processors for research project no. 3, the Region of Southern Denmark has not demonstrated that a decision has been taken on the level of supervision, and that the region's guideline for determining the level of supervision in that connection has been followed.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

On 9 October 2020, the Norwegian Data Protection Authority notified the Region of Southern Denmark that the Danish Data Protection Authority would carry out written supervision of the region's processing of personal data for research use. In this connection, the Danish Data Protection Authority requested to receive an overview of the region's ongoing research projects and an overview of the region's policies, procedures and guidelines.

On 30 November 2020, Region South Denmark sent an overview of the region's ongoing health science research projects and a more general record of the research area in the region kept in accordance with Article 30 of the Data Protection Regulation. Region South Denmark also sent a list of disclosures of information to other health science research projects outside the region.

Against this background, the Danish Data Protection Authority selected the following three projects within the subjects "processing basis" and "data responsibility and roles":

"Molecular screening for hereditary bowel cancer in Denmark" (local journal number 18/56894 in appendix 1), started on 1 January 2013,

"DaneSpine - Quality of life and technical results after spinal surgery" (local journal number 18/22987 in appendix 1), started on 1 November 2016 and

"Investigation of the vessel wall of cerebral aneurysms with a view to tensile strength and correlation to computer-calculated tensile strength" (local journal number 17/44503 in appendix 1), started on 1 January 2018.

It appeared from the region's overview that information was processed on e.g. health conditions in connection with all three projects, and that data processors were used.

On 19 February 2021, the Danish Data Protection Authority requested the Region of Southern Denmark for a range of information regarding the three projects, including information on the legal basis for the processing of the information in the projects, whether data processing agreements had been entered into, including when, whether there had been an update later, whether supervision had been carried out with the data processors, as well as whether the supervision had been carried out in accordance with the region's guideline "Conclusion of data processing agreements and supervision of data processors".

Furthermore, the Danish Data Protection Authority requested to receive a copy of the data processing agreements, documentation for any supervision of the data processors and the guideline "Conclusion of data processing agreements and supervision of data processors", which was listed on the region's list of policies, procedures and guidelines (in connection with a revision of the guideline in April 2021, its title has been changed to "Data processor agreements, supervision of data processors and confidentiality declarations", cf. below section 2.4.).

2.1.

The Region of Southern Denmark has stated in relation to research project no. 1 ("Molecular screening for hereditary bowel cancer in Denmark") that the personal data in the project is processed pursuant to Article 6, paragraph 1 of the Data Protection Regulation. 1, letter e, Article 9, subsection 2, letter j, and § 10 of the Data Protection Act[2].

In its consultation response of 19 March 2021, the Region of Southern Denmark stated that a data processing agreement was entered into on 15 November 2018 with the HNPCC register. The data processing agreement is still valid, but has not been updated. The HNPCC register has not yet been audited.

The following is inserted in the data processing agreement on supervisory authorities, audits and auditors' statements:

"7.1. The data processor must, at the Data Controller's request, provide the Data Controller with the necessary information so that the Data Controller can take care of the obligations under this agreement, including whether the mentioned technical and organizational security measures, etc. is taken. Furthermore, the Data Processor must be able to document that identified vulnerabilities are addressed based on a risk-based assessment.

7.2. In the event that the Data Controller and/or relevant public authorities, in particular the Danish Data Protection Authority, wish to carry out a physical inspection (audit) of the measures taken by the Data Processor in accordance with the Data Processor Agreement, the Data Processor undertakes - with reasonable notice - to time and resources available for this. The Data Processor undertakes in the same way to ensure that such audits can also be carried out at its Sub-Data Processors by the Data Processor.

7.3. As a supplement or alternative to the audits mentioned above, an agreement can be entered into that the Data Processor and any Sub-Data Processors, at their own expense, ensure that an independent expert prepares an annual audit statement based on a recognized standard regarding the Data Processor's compliance with the requirements for security measures set out in the Data Processor Agreement . The declaration must be formulated in relation to the task that the Data Processor solves for the Data Controller. An agreement to this effect must appear in section 15, unless otherwise stated in the main agreement."

It is noted that an agreement on an annual audit statement is not adopted in the data processing agreement's section 15.

2.2.

The Region of Southern Denmark has stated regarding research project no. 2 ("DaneSpine - Quality of life and technical results after spinal surgery") that the personal data in the project is processed pursuant to Article 6, paragraph 1 of the Data Protection Regulation. 1, letter e, and § 6 of the Data Protection Act. In addition, the health information is processed pursuant to Article 9, subsection of the Data Protection Act. 2, letter j, and Section 10 of the Data Protection Act. The processing of CPR numbers is based on Article 87 of the Data Protection Regulation and Section 11 of the Data Protection Act.

Furthermore, in March 2019, the Region of Southern Denmark stated that there are no longer any external data processors associated with the research project, as otherwise appears from the region's internal list of ongoing health science research projects. The system in which the information is stored was taken from the data processor to the region several years ago. In this connection, the Region of Southern Denmark has stated that the list will be updated accordingly.

2.3.

The Region of Southern Denmark has stated regarding research project no. 3 ("Investigation of the vessel wall of cerebral aneurysms with a view to tensile strength and correlation to computer-calculated tensile strength") that the personal data in the project is processed on the basis of the Committee Act and Section 10 of the Data Protection Act.

Region Southern Denmark has stated that there are two data processors associated with the research project. A data processing agreement was concluded with HD-Support ApS in April 2018, while a data processing agreement with the University of Southern Denmark was concluded in November 2020. For both data processing agreements, it applies that they have not been updated since the conclusion.

As far as HD-Support ApS is concerned, the Region of Southern Denmark has stated that an inspection has not yet been carried out, but that an inspection is planned to be carried out in the spring of 2021. The following has been inserted in the data processing agreement regarding supervisory authorities, audits and audit statements:

"The data processor must, at the Data Controller's request, provide the Data Controller with sufficient information to ensure that the mentioned technical and organizational security measures, etc. is taken. Furthermore, the Data Processor must be able to document that identified vulnerabilities are addressed based on a risk-based assessment.

In the event that the Data Controller and/or relevant public authorities, in particular the Danish Data Protection Authority, wish to carry out a physical inspection (audit) of the measures that the Data Processor undertakes pursuant to the Data Processor Agreement, the Data Processor undertakes - with reasonable notice - to time and resources available for this. The Data Processor undertakes in the same way to ensure that such audits can also be carried out at its Sub-Data Processors.

As a supplement or alternative to the audits mentioned above, an agreement can be entered into that the Data Processor and any sub-processors, at their own expense, ensure that an independent expert prepares an annual audit statement based on a recognized standard regarding the Data Processor's compliance with the requirements for security measures set out in the Data Processor Agreement . The declaration must be formulated specifically in relation to the task that the Data Processor solves for the Data Controller. An agreement to this effect can be found in point 15."

It is noted that an agreement on an annual audit statement is not adopted in the data processing agreement's section 15.

As far as the University of Southern Denmark is concerned, Region Southern Denmark has stated that it has been agreed in the data processing agreement that inspections must be carried out every three years, and that this has not yet been carried

out. The following is inserted in the data processing agreement on supervision and audit:

"7.1. The Data Processor makes all information necessary to demonstrate the Data Processor's compliance with the Data Protection Legislation and the Data Processor Agreement available to the Data Controller and enables and contributes to audits, including inspections, carried out by the Data Controller or another auditor authorized by the data controller.

7.2. The following supervision has been agreed in the Data Processor Agreement. The Data Processor must answer and fill in a questionnaire prepared by the Data Controller every 3 years free of charge. The data controller or a representative of the data controller has the right to ask further questions to the Data Processor at any time, when, according to the data controller's factual assessment, a need for this arises.

2.4.

The Region of Southern Denmark has drawn up the guideline "Data processor agreements, supervision of data processors and confidentiality declarations", from which it appears that determining the form and frequency of supervision of the data processor must take place on the basis of a risk assessment, which must also form the basis for entering into the data processor agreement. According to the guidelines, inspections should generally be carried out once a year.

The guideline was last revised in April 2021, according to the document's change log. Region Southern Denmark has stated that it is primarily the wording and appearance of the guideline that was revised. The Danish Data Protection Authority must then assume that the section on determining the level of supervision was also specified in the guideline before April 2021.

Region Southern Denmark has generally stated regarding data processing agreements that the region will initiate work in relation to the preparation of specific supervisory material for the relevant project managers in addition to the already existing material in the region. The supervision material is targeted at the research area, as the region is aware that supervision is a major task for the relevant project managers. The inspection material will regulate both written and physical inspections.

3. Reason for the Data Protection Authority's decision

It follows from the data protection regulation's article 9, subsection 1, that a ban on the processing of information covered by Article 9 of the regulation, including health information, applies as a general rule. However, the prohibition does not apply if one of the exceptions in the data protection regulation, Article 9, subsection 2, letter a-j, is fulfilled.

According to the data protection regulation's article 9, subsection 2, letter j, processing of sensitive information is covered by Article 9, subsection 1, legal, i.a. if processing is necessary for scientific or historical research purposes or for statistical

purposes in accordance with Article 89, paragraph 1, on the basis of EU law or the national law of the Member States and is proportionate to the objective pursued, respects the essential content of the right to data protection and ensures appropriate and specific measures to protect the fundamental rights and interests of the data subject.

It also follows from § 10, subsection of the Data Protection Act. 1, that information as mentioned in the data protection regulation, article 9, subsection 1, may be processed if this is done solely for the purpose of carrying out statistical or scientific studies of significant societal importance, and if the processing is necessary for the purpose of carrying out the studies.

3.1. Regarding research project no. 1 and no. 2

As the information was processed in connection with research projects at Region Southern Denmark, which must therefore be considered scientific studies of significant societal importance, the Danish Data Protection Authority finds that the processing of information in connection with research projects no. 1 and no. 2 could take place within the framework of the data protection regulation's article 9, subsection 2, letter j, cf. the Data Protection Act § 10, subsection 1, and the data protection regulation article 6, subsection 1, letter e.

As far as research project no. 2 is concerned, the authority for processing the CPR number is stated to be Article 87 of the Data Protection Regulation and Section 11 of the Data Protection Act, which does not give the Data Protection Authority cause for comments.

3.2. Regarding research project no. 3

The Danish Data Protection Authority finds no basis for overriding Region Southern Denmark's assessment that the processing of the information in research project no. 3 could take place on the basis of the committee act, cf. the data protection regulation, article 9, subsection 2, letter j, and § 10 of the Data Protection Act.

3.3. Data processor agreements

As far as research project no. 2 is concerned, Region Southern Denmark has stated that there are no longer any external data processors associated with the research project, as the system where the information is stored was taken over several years ago.

The Danish Data Protection Authority finds it inappropriate that, at the time of the consultation with the region, it appeared from the region's internal register of ongoing health science research projects that data processors were used. The inspection assumes that the list is now up to date.

In connection with research project No. 1 and No. 3, the Region of Southern Denmark entered into data processing agreements with three different data processors in 2018 and 2020, respectively, and the agreements have not been subsequently updated. This does not give rise to comments by the Data Protection Authority.

3.4. Supervision of data processors

The Danish Data Protection Authority is of the opinion that a data controller must ensure the processing security of its data processors. This is because the data controller must meet the requirement for accountability in Article 5 of the Data Protection Regulation and must thereby be able to demonstrate that a processing of personal data is in accordance with the rules of the Data Protection Regulation. In the opinion of the Data Protection Authority, the data controller will not be able to meet the above requirements by simply entering into a data processing agreement with the data processor. The data controller must therefore also carry out a (larger or smaller) supervision to ensure that the entered data processing agreement is complied with, including that the data processor has implemented the agreed technical and organizational security measures.

Regarding research project no. 1, the Danish Data Protection Authority notes that a level of supervision is not stipulated in the data processor agreement with the HNPCC register, but that Region Southern Denmark in its guideline "Data processor agreements, supervision of data processors and confidentiality statements" has stated that supervision of the data processor should, as a starting point, be carried out once yearly. The Region of Southern Denmark has, however, stated in March 2021 that there has been no supervision of the data processor.

Regarding research project no. 3, the Danish Data Protection Authority notes that a level of supervision is not stipulated in the data processing agreement with HD-Support ApS, but that Region Southern Denmark has stated that an inspection was intended to be carried out in the spring of 2021.

Regarding research project no. 3, Region Southern Denmark has, according to the data processor agreement with the University of Southern Denmark, to carry out an inspection of the data processor once every three years. The fact that the data processor has not been supervised does not give rise to observations by the supervisory authority, as the data processor agreement was only entered into in November 2020.

The Danish Data Protection Authority, however, finds reason to criticize the fact that, with regard to the data processing agreement for research project no. 1 and the data processing agreement with HD-Support ApS for research project no. 3, the Region of Southern Denmark has not demonstrated that a decision has been taken on the level of supervision, and that the

region's guideline for determining the level of supervision in that connection has been followed.

In the above decision, the Danish Data Protection Authority has not otherwise made a further determination as to whether the level of supervision for data processors set by the Region of Southern Denmark was appropriate.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).