Supervision of the Capital Region's processing of personal data for research use

Date: 16-02-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Data processor

Sensitive information

The Danish Data Protection Authority has carried out a planned written inspection at the Capital Region with a focus on the subjects of processing grounds and data responsibility.

Journal Number: 2020-422-0025

Summary

In autumn 2020, the Norwegian Data Protection Authority decided to supervise a number of activities in the research area. The Capital Region was among the authorities the Data Protection Authority selected for a written inspection.

In connection with the inspection, the Danish Data Protection Authority received a list of ongoing research projects at the Capital Region as well as the region's policies, procedures and guidelines regarding data protection. On this basis, the Norwegian Data Protection Authority selected three research projects as the subject of the investigation within the subjects "processing basis" and "responsibility and roles (data responsibility)".

The Norwegian Data Protection Authority found no basis for overriding the Capital Region's assessment of the basis for the processing of personal data in the three projects. In addition, the inspection found that data processing agreements had been entered into.

However, the supervisory body criticized the fact that the Capital Region had not carried out sufficient supervision in one of the projects within the framework of the level of supervision the region had found appropriate. The inspectorate also found it critical that in another project the region had not followed the region's own model for determining the level of supervision.

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 Capital Region has entered into data processing agreements with the data processors for the research projects, and these have not been subsequently updated. This does not give rise to comments by the Data Protection Authority.

However, the Danish Data Protection Authority finds occasion to express criticism that the Capital Region, as far as the data processor for the 2nd research project is concerned, has not conducted supervision within the framework of the level of supervision that the region had found appropriate, and that the region, as far as the data processor agreement for the 3rd. research project has not followed the region's model for determining the level of supervision, and that, moreover, it has not been demonstrated that a decision had been taken on the level of supervision.

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 Data Protection Authority notified the Capital Region that the Data Protection Authority would carry out written supervision of the region's processing of personal data for research use. In this connection, the Norwegian Data Protection Authority requested, among other things, to receive an overview of the region's ongoing research projects and an overview of the region's policies, procedures and guidelines.

The Capital Region forwarded on 27 November 2020 i.a. an overview of the region's ongoing research projects, and on this basis the Danish Data Protection Authority selected the following three projects within the subjects "processing basis" and "data responsibilities and roles"

"Efficacy of seven and fourteen days of antibiotic treatment in uncomplicated Staphylococcus aureus infection", started on 23 August 2017

"Health predictors and consequences of inflammatory bowel disease and microscopic colitis", started on 1 October 2018

"Screening for the significance of epigenetic changes for T1D development", started on 1 March 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.

In connection with the three research projects, the Danish Data Protection Authority requested the region for information regarding the legal basis for the processing of information in the projects, whether data processing agreements had been entered into, including when, whether updates had subsequently taken place, and whether the data processors had been

supervised.

The Danish Data Protection Authority also requested to receive a copy of the data processor agreements, documentation for any supervision of the data processors as well as the Capital Region's policy called "Model for supervision of external data processors".

The document "Model for supervision of external data processors" is a description of the region's procedure for assessing which level of supervision a data processor must be subject to. It is described that the level of supervision must be assessed on the basis of a risk assessment, where emphasis is placed on the following parameters: supervision complexity, the personal attribution of the information (i.e. whether the information is pseudonymised), the number of registered persons and the level of confidentiality (i.e. the nature of the information and whether is general or sensitive information).

The region has prepared an excel sheet where the data processor is scored from 1 (low) to 5 (high) on the various parameters, and on the basis of this, an overall risk score is calculated. Based on the risk score, a supervision level of either, low, medium, high or very high is assigned, which indicates what type of supervision must be carried out and how often supervision must be carried out. If the person responsible for supervision has reason to question this level of supervision, a concrete risk assessment must, however, be carried out.

2.1.

The Capital Region has stated regarding the 1st research project that the research project is a clinical drug trial, which is carried out on the basis of Article 6, paragraph 1 of the Data Protection Regulation. 1, letter e, Article 9, subsection 2, letter j, as well as the Committee Act and the Medicines Act.

This appears from section 2.4.1.2.1 of the proposal for an act on scientific ethical treatment of clinical trials of medical equipment etc. (L 159), that the Medicines Act, the Committee Act and the GCP order form the legal basis for the researchers' processing, including the collection of personal data in connection with clinical trials with medicinal products for use for research purposes and with a view to fulfilling the legal obligations incumbent on the researcher, regardless that the said legal bases do not contain actual data protection legal rules.

The current clinical drug trials are covered by the Medicines Act, the Committee Act and the GCP order, as it is a clinical trial with drugs where the drug in question is tested on humans. It appears from the specific national legal basis that such trials are covered by the laws' scope of application - and for both the Committee Act and the Medicines Act, there is a definite duty to

notify.

It is therefore the opinion of the Capital Region that the Medicines Act, the Committee Act and the GCP order together constitute the national legal basis, which in conjunction with Article 9, subsection 2, letter j, forms the basis for the processing of personal data in connection with the relevant clinical drug trial.

The research project began on 23 August 2017, and the region has stated that it is generally a project where new inclusion sites and external parties are continuously added.

After the start of the project, a center in Brazil – Pontifícia Universidade Católica do Parana – was included, which was to contribute to the data processing. The Brazilian site was only added to the project when it became relevant and allowed to include patients from Brazil in the project, and the data processing agreement was therefore also only concluded on 3 November 2020. The agreement has not been updated subsequently.

The Capital Region has further stated that the region has not yet supervised the data processor. The level of supervision is determined in accordance with the Capital Region's model for supervision of external data processors, and a questionnaire will therefore be sent continuously and at least every three years, to which the data processor must answer.

The following is inserted in the data processing agreement on supervision:

"The Data Processor shall at the request from the Data Controller complete a questionnaire regarding the compliance of the Data Processing Agreement. The questionnaire will contain approximately 10 questions, drawn up by the Data Controller. The agreed audit level does not prevent the Data Controller from carrying out a separate audit in accordance with the Data Processing Agreement clause 7.1."

2.2.

The Capital Region has stated in relation to the 2nd research project that it is a register research project that is carried out pursuant to Article 6, paragraph 1 of the Data Protection Regulation. 1, letter e, article, 9, subsection 2, letter j, and the Data Protection Act[2] § 10, subsection 1.

On 19 June 2019, the Capital Region entered into a framework data processing agreement with Statistics Denmark, which replaced the previous framework agreement that was concluded between the parties on 23 February 2015. This is an overarching agreement regarding the Capital Region's use of the research machine at Statistics Denmark. The agreement was not subsequently updated.

In consideration of the regions' resources and to ensure that all five regions do not supervise the same supplier at the same time, the regions decided to carry out joint supervision of a number of data processors that all the regions used. One region was therefore appointed supervisor on behalf of the other regions for the selected systems.

Since all five regions use Statistics Denmark's research service, Region Southern Denmark has carried out the supervision of Statistics Denmark's research service on behalf of the regions. The inspection was carried out in the period 27 November 2020 to 4 March 2021 as a written inspection in the form of obtaining an external audit statement of the ISAE 3000 type in accordance with the data processing agreement. The Capital Region has sent documentation for this.

The following appears from the data processing agreement regarding supervision:

"The data processor makes all information necessary to demonstrate the data processor's compliance with Article 28 of the Data Protection Regulation and this agreement available to the data controller. This is done by the data processor annually making an external audit statement available to the data controller."

The level of supervision was set before the Capital Region's model for supervision of external data processors was drawn up.

2.3.

The Capital Region has stated in relation to the 3rd research project that the research project is a health science intervention study, which is carried out pursuant to Article 6, paragraph 1 of the Data Protection Regulation. 1, letter e, Article 9, subsection 2, letter j, section 10, subsection of the Data Protection Act. 1, and the committee act.

On 30 January 2020, the Capital Region entered into a data processing agreement with Lund University Diabetes Centre. The agreement was not subsequently updated.

The data processor's task was only relevant after the data collection for the research project had been completed, as the data processor's task was to analyze the biological material from the project. The data processing agreement was therefore only concluded on 30 January 2020, even though the project itself started on 1 March 2018.

The Capital Region has not supervised the data processor. The wording of the level of supervision in the data processor agreement does not follow the region's model for supervision of external data processors, as the data processor agreement is concluded on an older version of the region's data processor agreement template. The following is inserted in the data processing agreement on supervision:

"At the request of the Data Controller, the Data Processor shall provide the Data Controller with necessary information to

enable the Data Controller to supervise the obligations according to the present Data Processing Agreement, including whether the above technical and organizational security measures, etc., have been taken Furthermore, the Data Processor shall document that identified vulnerabilities are met on the basis of a risk-based assessment.

If the Data Controller and/or the relevant public authorities, in particular the Data Protection Agency, wants/want to carry out a physical inspection (audit) of the measures taken by the Data Processor according to the Data Processing Agreement, the Data Processor undertakes – with a reasonable notice – to make time and resources available for this purpose. Similarly, the Data Processor undertakes to ensure that such audits can also be carried out by the Data Processor at his Sub-Processors."

3. Reason for the Data Protection Authority's decision

3.1. Basis of treatment

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.

The following appears from the comments on the proposal for an act on scientific ethical treatment of clinical trials of medical equipment, etc. [3]:

"It follows from section 3, subsection of the committee act. 3, that the subject's consent to participation in a clinical trial with medicinal products gives the sponsor, the sponsor's representatives and the investigator direct access to obtain information in patient records, etc., including electronic records, in order to see information about the subject's health conditions, which is necessary as part of implementation of the research project, including quality control and monitoring, which they are obliged to carry out.

It also follows from section 89, subsection of the Pharmaceuticals Act. 3, that a consent given in accordance with the Personal Data Act (today the Data Protection Act) gives the sponsor and the sponsor's representatives and investigator direct access to

obtain information in patient records etc., including in electronic records, in order to see information about the subject's health conditions, which is necessary as part in the implementation of the research project, including quality control and monitoring, which they are obliged to carry out.

A sponsor is a natural or legal person who assumes responsibility for the initiation, management or financing of a health science research project that e.g. concerns clinical trials with medicinal products, cf. section 2, no. 6 of the committee act.

The sponsor's representative is a monitor who, in accordance with Section 2, No. 14, Section 5, No. 3 of the Committee Act, as well as Sections 15 and 16 of Executive Order No. 695 of 12 June 2013 on good clinical practice in connection with clinical trials with medicinal products on humans (hereinafter the GCP order), must ensure that the data collected in the trial are robust and reliable. Sponsor appoints monitor.

Investigator (pursuant to section 2 of the Committee Act, no. 6, defined as trial manager) is a person who is responsible for the practical implementation of the trial at a specific trial site.

Section 3 of the Committee Act, subsection 3, and Section 89(1) of the Medicines Act. 3, regulates only when the sponsor, the sponsor's representatives and the investigator can obtain patient record information - i.e. the electronic retrieval access itself, and not the other processing of personal data that takes place in connection with a clinical trial with medicinal products.

It also follows from Section 3, subsection of the Committee Act. 4, that the consent to participation in a health science research project which, among other things, concerning clinical trials with medicinal products, can be revoked at any time without this being detrimental to the subject. A revocation does not affect the right to process personal data that has already been included in the research project about the subject in question.

In addition, the Medicines Act and the Committee Act contain provisions on when the sponsor/investigator will be legally obliged to process personal data.

This follows, for example, from Section 30(1) of the Committee Act. 1, that the sponsor or the person in charge of the trial must immediately notify the supervisory committee if, during the implementation of a health science research project, which i.a. regarding clinical trials with medicinal products, suspected serious unexpected side effects occur as a result of the project. It also follows from section 89, subsection of the Pharmaceuticals Act. 2, no. 1, that the sponsor must immediately notify the Danish Medicines Agency if unexpected and serious suspected side effects occur during the trial.

It also follows from §§ 17 and 18 of the GCP order that the sponsor and investigator must prepare and store a master file for

the clinical trial. The purpose of the master file is to conduct the clinical trial and for the Danish Medicines Agency to continuously assess the quality of the data produced, including whether the sponsor and investigator have complied with the principles and guidelines for good clinical practice.

The master file contains, for example, information about the test subjects in the form of signed consent and power of attorney statements as well as reporting of side effects from the investigator to the sponsor, cf. appendix 2 of the GCP order.

The Medicines Act, the GCP order and the committee act thus require the processing of personal data about the test subjects as part of participation in a clinical trial, and thereby the said laws and the GCP order constitute the legal basis for the researcher's treatment, including the collection of personal data in connection with clinical trials with medicines for use for research purposes and with a view to fulfilling the legal obligations incumbent on the researcher, regardless of the fact that the mentioned legal bases do not contain actual data protection legal rules. The Medicines Act, the GCP order and the committee act are maintained within the framework of the data protection regulation, article 9, subsection 2, letter j, cf. the Ministry of Justice's report no. 1565 on the data protection regulation, part II, page 61 f. For a more detailed review of the data protection legal rules, refer to section 2.4.1.1. above about the Data Protection Act and the Data Protection Regulation."

Based on this, the Data Protection Authority finds no reason to override the Capital Region's assessment that the processing of the information in connection with the clinical trial with medicinal products (1st research project) could take place on the basis of Article 9, subsection 1, letter j, cf. the Medicines Act, the GCP order and the committee act and at the same time the data protection regulation article 6, subsection 1, letter e.

This follows from Section 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.

Since the information was processed in connection with research projects at the Capital Region and thus must be considered scientific studies of significant societal importance, the Danish Data Protection Authority finds that the processing of information in connection with the 2nd and 3rd research projects could take place within the framework of Article 9, paragraph 1 of the Data Protection Regulation . 2, letter j, cf. the Data Protection Act § 10, subsection 1, and at the same time the data protection regulation article 6, subsection 1, letter e.

3.2. Data processor agreements

In connection with all three research projects, the Capital Region has entered into data processing agreements in either 2019 or 2020 with the various data processors, and the agreements have not been subsequently updated. This does not give rise to comments by the Data Protection Authority.

3.3. 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 (larger or smaller) supervision to ensure that the concluded data processor agreement is complied with, including that the data processor has implemented the agreed technical and organizational security measures.

In relation to the 1st research project, the Danish Data Protection Authority notes that, based on its model for supervision of data processors, the region has assessed that inspections must be carried out every three years, and it therefore does not give the authority reason to comment that the data processor has not been supervised, as the data processing agreement was only entered into on 3 November 2020.

With regard to the 2nd research project, the Capital Region has assessed, based on its model for supervision of data processors, that the data controller should provide an external audit statement once a year to show that the data processor complied with Article 28 of the regulation and the data processor agreement in general.

The Danish Data Protection Authority notes that the regions have chosen to carry out inspections jointly, and that in the period from 27 November 2020 to 4 March 2021, Region Southern Denmark carried out written inspections of the data processor on behalf of all the regions. Thus, for the Capital Region, no annual supervision of the data processor is seen, as the Capital Region entered into the data processing agreement on 19 June 2019.

Regarding the 3rd research project, the Danish Data Protection Authority notes that the Capital Region has stated that the formulation of the level of supervision in the data processor agreement does not follow the region's model for supervision of external data processors, as the data processor agreement was concluded on an older version of the region's data processor agreement template. Furthermore, there is no further information on the level of supervision, either in the data processing

agreement or in connection with the present supervision. The Danish Data Protection Authority thus does not find it proven that a decision has been taken on the level of supervision.

In summary, the Danish Data Protection Authority finds occasion to express criticism that the Capital Region, as far as the data processor for the 2nd research project is concerned, has not conducted supervision within the framework of the level of supervision that the region had found appropriate, and that the region, as far as the data processor agreement for the 3rd. research project has not followed the region's model for determining the level of supervision, and that, moreover, it has not been demonstrated that a decision had been taken on the level of supervision.

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

[3] L 159 Proposal for an Act on scientific ethical treatment of clinical trials of medical equipment etc., section 2.4.1.2.1 (Reproduced by L 62 Proposal for an Act on scientific ethical treatment of clinical trials of medical equipment etc., section 2.4.1.2.1 )