Supervision of the Danish Health Data Agency's supervision of two data processors

Date: 16-12-2022

Decision

Public authorities

No criticism

Supervision / self-management case

Data processor

Basic principles

The Danish Health Data Agency's supervision of two data processors did not give rise to criticism.

Journal number: 2021-421-0100

Summary

The Norwegian Data Protection Authority has carried out a written inspection of the Danish Health Data Agency's supervision of two of the agency's data processors.

The Danish Data Protection Authority found no reason to override the Danish Health and Data Protection Agency's assessment that the agency's supervision of Medcom and Netcompany IT and Business Consulting A/S in the form of annual collection of audit statements - and determination of any measures to the extent that review of the statements gives rise to this - constitutes appropriate supervision of the data processors.

Decision

1. Written supervision of the Danish Health Data Agency's supervision of data processors

The Danish Health Data Protection Agency was among the authorities that the Danish Data Protection Authority had selected in the autumn of 2021 to supervise according to the data protection regulation[1] and the data protection act[2].

The Danish Data Protection Authority's inspection was a written inspection, which focused on the Danish Health and Data Protection Agency's inspection of data processors.

By letter of 9 November 2021, the Danish Data Protection Authority notified the Danish Health Data Protection Agency. In this connection, the Danish Data Protection Authority requested to be sent a list of data processors to whom the Danish Health and Data Protection Agency entrusts sensitive and/or confidential information.

The Danish Health Data Agency published a list of the agency's data processors on 29 November 2021.

On the basis of the list, the Danish Data Protection Authority chose to carry out an inspection of the Danish Health Data Agency's supervision of the agency's data processors Medcom and Netcompany IT and Business Consulting A/S (hereafter Netcompany).

On 8 December 2021, the Norwegian Data Protection Authority requested the Danish Health Data Agency to provide information on:

the board's plan for its supervision of Medcom and Netcompany, including considerations about frequency and what is being supervised

whether the agency has supervised Medcom and Netcompany

how the agency has followed up on any completed inspections of Medcom and Netcompany.

On that basis, the Danish Health Data Agency sent a statement on the matter on 17 January 2022.

2. Decision

After a review of the case, the Danish Data Protection Authority finds no basis for overriding the Danish Health Data Agency's assessment that the agency's supervision of the data processors Medcom and Netcompany has taken place in accordance with the rules in the data protection regulation, article 5, subsection 2, cf. subsection 1.

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

3. Case presentation

It appears from the case that Medcom processes personal data on behalf of the Danish Health Data Agency when operating the Health Data Network, including:

National notification service

Treatment Relationship Service

Security Token System (ticket exchange)

My log

Consent Service

Common Family Card

Common Medicine Card

Agreements

Plans and efforts

Data collection, adaptation, development, processing and validation of data at DAKI

Closed e-Health: dissemination of data for municipal planning needs

The health platform.

It also appears from the case that Netcompany processes personal data on behalf of the Danish Health Data Agency for support, troubleshooting and further development of the systems eHealth, SOR, Forskerservice and Evaluation of rational clinics.

The Danish Health Data Agency has stated that the agency almost always processes confidential and sensitive personal data (e.g. social security numbers and health information). The processing is critical for the data subjects and therefore requires a higher degree of control, which is best achieved through regular supervision. This also applies in relation to the two selected data processors, Medcom and Netcompany.

The Danish Health Data Agency has therefore chosen and made it in writing in a supervisory procedure that, in connection with the supervision of the agency's data processors, an ISAE3000 statement is always obtained as a starting point, which relates to the processing of personal data. The Danish Health Data Agency has also assessed that this supervision procedure is in good line with the Danish Data Protection Authority's guidance on supervision of data processors from October 2021.

Furthermore, the Danish Health Data Agency has stated that the background for this choice is that ISAE3000 declarations provide a good connection between treatment and declaration – one of the highest degrees of security beyond real inspections. It is also associated with a markedly lower resource draw at both the Danish Health Data Agency and the data processor, which gives the agency the opportunity to carry out inspections with a higher cadence, which in turn provides higher security.

For the two selected data processors, an annual inspection is basically carried out, as they process sensitive and/or confidential personal data. Both data processors submit an ISE3000 audit statement prepared by an impartial auditor. Netcompany has also submitted an ISAE3402 declaration.

As far as what is being supervised, the Danish Health Data Agency has stated that when reviewing the ISAE3000 declaration, it is followed up on whether the declaration relates to the data processing agreements entered into by the Danish Agency and

compliance with the requirements therein, as well as a comparison with observations from previous year's inspection. The Danish Health Data Agency uses an internal template for the review, which ensures that it is uniform and appropriate. In addition, the supervision can be shaped according to relevant themes or on the basis of concrete incidents.

In addition, the Danish Health Data Agency has stated that the agency has supervised Medcom and Netcompany. The supervision is initially carried out by the agency's information security department. This has happened by reviewing audit statements for both data processors and in certain cases by communicating with the data processors to clarify e.g. the scope of the declaration and the nature of the controls. After the review, the Danish Health Data Agency prepares an internal inspection report, which the agency, among other things, used in the subsequent inspection to ensure coherence between the inspections and follow-up on any audit comments.

For Medcom, the Danish Health Data Agency has most recently received and reviewed an ISAE3000 type II audit statement for the period 2020, carried out by an external and impartial auditor. The declaration was not specifically prepared for the Danish Health Data Agency, but the review showed that there was a 1-1 correlation between the declaration and the service that the Danish Health Data Agency receives. The inspection with Medcom has been completed, and an internal inspection report has been prepared on 11 November 2021. Previous inspections were carried out on 4 March 2020 (declaration relating to 2018). The Danish Health Data Agency also received a statement for the processing in 2019, which was also reviewed.

For Netcompany, the Danish Health Data Agency has most recently received and reviewed an ISAE3000 type II statement and an ISAE3402 statement for the period 2020, both of which were carried out by an external and impartial auditor. ISAE3402 is a general declaration, but the Danish Health Data Agency assessed that there was an appropriate connection between the declaration and the treatment. The inspection of Netcompany has been completed, and an internal inspection report has been prepared on 24 June 2021.

The Danish Health Data Agency has stated that, for the two selected data processors, the inspection was based on a review of the audit statements received as well as the agency's internal inspection report for the previous inspections. The internal supervision reports, which are prepared after the review of the audit statements, have also been sent for information to the Danish Health Data Agency's system administrators, so that they are aware of any concerns. If the inspection gives cause for concern or it is assessed that further inspection measures are necessary, these will be carried out. However, it has not been necessary with Medcom and Netcompany.

The Danish Health Data Agency has also stated that, for Medcom, the auditor's observations in the ISAE3000 statement for 2018 were not of a critical nature, and the data processor's plan for accommodation and countermeasures appeared reasonable. The Danish Health Data Agency followed up on the observations in connection with the following year's audit statements for the treatment in 2019 and again in 2020. Here it was checked whether the observations had been closed or whether there was reasonable progress in relation to solving them, which the agency has assessed that there was.

For Netcompany, the auditor's observations in the ISAE3000 statement for 2020 were also not of a critical nature. The Danish Health Data Agency has stated that a new declaration will be obtained in the 1st quarter of 2022, after which it will be investigated whether the previously stated observations have been taken care of, or whether further follow-up is required.

In conclusion, the Danish Health Data Agency has stated that the agency reviews the audit statements internally, and that on that basis it is assessed whether and, if applicable, which measures should be implemented.

4. Reason for the Data Protection Authority's decision

It follows from the data protection regulation article 28, subsection 1, that a data controller may only use data processors who can provide the necessary guarantees that they will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of the data protection regulation and ensures protection of the data subject's rights.

Of the data protection regulation, article 24, subsection 1, it appears that the data controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is in accordance with the regulation.

The data controller must thus be able to demonstrate that the data processor provides sufficient guarantees for the implementation of technical and organizational measures that meet the requirements of the data protection regulation and ensure protection of the data subject's rights. This detection must be possible throughout the treatment process over time, which i.a. can be done by controls.

This appears from the data protection regulation's article 5, subsection 1, letter a, that personal data must be processed legally, fairly and in a transparent manner in relation to the data subject ("legality, fairness and transparency").

Furthermore, it follows from the regulation's article 5, subsection 1, letter f, that personal data must be processed in a way that ensures sufficient security for the personal data in question, including protection against unauthorized or illegal processing and

against accidental loss, destruction or damage, using appropriate technical and organizational measures ("integrity and confidentiality").

In addition, it follows from the data protection regulation article 5, subsection 2, that the data controller is responsible for and must be able to demonstrate that Article 5, subsection 1, is observed.

Article 5, subsection 2, contains an accountability principle which – in the Danish Data Protection Authority's view – means that the data controller must ensure and be able to demonstrate that personal data is processed for lawful and reasonable purposes and that the data is processed in a way that ensures sufficient security for the personal data in question – also when the data controller asks another party (a data processor or sub-processor) to process the information on its behalf.

Lack of follow-up on the processing of personal data by data processors and sub-processors will – in the opinion of the Danish Data Protection Authority – basically mean that the data controller cannot ensure or demonstrate that the processing complies with the general principles for the processing of personal data, including that the data is processed on a legal, fair and transparent manner in relation to the data subject ("lawfulness, fairness and transparency"), and that the information is processed in a way that ensures sufficient security for the personal data in question, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

In October 2021, the Danish Data Protection Authority published new, practically applicable guidance on how data controllers can carry out such inspections[3]. It appears from the guidance that the greater the risks there are for the data subjects in the processing by the data processor, the greater the demands placed on the data controller's supervision of the data processor. This applies both in relation to how the data controller must carry out supervision and how often this must take place.

The guidance further states that supervision based on a statement prepared by an independent third party is a way for the data controller to carry out appropriate supervision when the data processor processes sensitive or confidential information about many data subjects on behalf of the data controller.

It also appears from the guidance that the data controller in that connection, i.a. must ensure that the supervision covers the processing activities of the data controller at the data processor.

After a review of the case, the Danish Data Protection Authority finds no basis for overriding the Danish Health Data Agency's assessment that the agency's supervision of the data processors Medcom and Netcompany has taken place in accordance

with the rules in the data protection regulation, article 5, subsection 2, cf. subsection 1.

The Danish Data Protection Agency has thereby emphasized that the Danish Health Data Agency has supervised the data processors Medcom and Netcompany by obtaining ISAE3000 statements prepared by external and impartial auditors, that the Danish Health Data Agency has reviewed the statements, prepared internal supervisory reports and followed up on previous observations, and that the Danish Health Data Agency has followed on whether the declaration relates to the data processing agreements entered into by the Agency and compliance with the requirements therein.

The Danish Data Protection Authority has also emphasized that the Danish Health Data Agency has supervised the agency's data processors Medcom and Netcompany annually, and that the agency has assessed the frequency of the inspections on the basis that the data processors process confidential and sensitive personal data on a large number of registered persons on behalf of the agency.

The Danish Data Protection Authority thus finds no reason to override the Danish Health Data Agency's assessment that the agency's supervision of Medcom and Netcompany in the form of annual collection of ISAE3000 auditors' declarations - and determination of any measures to the extent that a review of the declarations gives rise to this - constitutes appropriate supervision of the data processors.

[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] The Norwegian Data Protection Authority's guidance on supervision of data processors.