Supervision of the Tax Administration's supervision of a data processor

Date: 15-12-2022

Decision

Public authorities

No criticism

Supervision / self-management case

Data processor

Basic principles

The tax administration's supervision of a data processor did not give rise to criticism.

Journal number: 2021-421-0099

Summary

The Danish Data Protection Authority has carried out a written inspection of one of the Debt Agency's data processors. The Development and Simplification Agency (UFST), which belongs to the Tax Administration, has informed the Danish Data Protection Authority that the Debt Agency is part of the Tax Administration, which is one overall data controller. In addition, UFST has stated that UFST handles the task of supervising data processors.

The Danish Data Protection Authority found no reason to override UFST's assessment that the supervision of the data processor in the form of annual collection of audit statements followed by a review and follow-up thereon constitutes appropriate supervision of the data processor.

It also appears from the Danish Data Protection Authority's guidance on supervision of data processors that supervision based on a statement prepared by an independent third party is a way in which the data controller can carry out appropriate supervision when the data processor processes sensitive or confidential information about many data subjects on behalf of the data controller.

Decision

1. Written supervision of the Debt Agency's supervision of data processors

The Debt Agency was among the authorities that the Danish Data Protection Authority had chosen to supervise in autumn 2021 in accordance with the Data Protection Regulation[1] and the Data Protection Act[2].

The Danish Data Protection Authority's supervision was a written supervision which focused on the Debt Agency's supervision of data processors.

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

By letter of 30 November 2021, the Development and Simplification Agency (hereafter UFST) stated that the Debt Agency and the Development and Simplification Agency are part of the Tax Administration, which is one unified data controller. It appears from the letter that it is UFST's assessment that some of the data processing agreements entered into by the former SKAT as well as the Implementation Center for Recovery or the Tax Administration could be of relevance to the supervision.

The Danish Data Protection Authority stated by e-mail of 22 February 2022 that the Danish Data Protection Authority had understood the inquiry from UFST to mean that the Tax Administration is the data controller for the processing of personal data that takes place at the Debt Agency. The Danish Data Protection Authority therefore asked for a list of data processors at the Tax Administration, which relate to the Debt Agency, and where sensitive and/or confidential information is entrusted.

The Debt Agency came out on 14 July 2022 with a list of the agency's data processors.

Based on the list, the Danish Data Protection Authority chose to carry out an inspection of the Debt Agency's supervision of the agency's data processor Netcompany.

On 15 July 2022, the Danish Data Protection Authority requested the Debt Agency to provide information on whether:

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

whether the agency has supervised Netcompany

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

UFST has stated by letter of 26 August 2022 that UFST (which is an agency in the Tax Administration) handles the task of supervising compliance with data processing agreements in the area of the Tax Administration, which is why UFST has responded to the Data Protection Authority's letter.

On this basis, UFST sent a statement on the matter on 26 August 2022.

2. Decision

After a review of the case, the Danish Data Protection Authority finds no basis for overriding the UFTST's assessment that the

supervision of the data processor 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

The Debt Agency has stated by letter of 14 July 2022 that the agency is the arrears recovery authority for a large number of public creditors. For recovery, two programs are used. One system, DMI, is facing phasing out as claimants and claims are transferred to the other system, PSRM.

The data processor Netcompany is associated with the PSRM system. The purpose of the processing of the personal data is generally to deliver and operate the recovery system. The Debt Agency entrusts the following information to Netcompany:

name, address and social security number

information about children and marital status

income conditions, including information on wages, capital income, assets, private debt and interest as well as public transfers

arrears of tax, family benefits or other amounts that can potentially be offset against the nature of the debt, including whether the debt is related to a criminal offense (fines or court costs)

all payments and non-payments on the debt

information about joint debts and liabilities

information about dunning notices and other recovery steps that have been initiated against debtors

transport agreements with private creditors

information about health conditions, including e.g. information about medication consumption

The information mainly concerns debtors and creditors. In addition, information about the debtor's spouse, children, guardians, lawyers etc. is processed.

The Swedish Debt Agency has stated that Netcompany, on behalf of the Swedish Debt Agency, carries out the following processing of personal data: Collection, registration, systematization, storage, change, search, use, passing on, entrustment, profiling, compiling or merging, including for control purposes, deletion and blocking or destruction.

UFST has stated by letter of 26 August 2022 that UFST in the Tax Administration handles the task of overseeing compliance with data processing agreements, which is why UFST has responded to the Data Protection Authority's letter.

UFST has stated that the agency annually implements a process for supervision of data processors. The assessment of whether the individual data processing agreement is supervised is based on the risk to the data subjects, and UFST has also identified some large and significant suppliers that the agency has chosen to supervise each year. Netcompany is one of them. The inspection includes an assessment of the supplier's compliance with the data processing agreement.

In addition, the UFST has stated that Netcompany's compliance with the data processing agreement has been monitored in 2021. The monitoring has taken place on the basis of two audit statements, respectively a general ISAE3000 statement and a specific ISAE3402 statement.

After reviewing the two audit statements, UFST has asked Netcompany some follow-up questions, which Netcompany has answered satisfactorily. The inspection is then completed on 1 July 2022.

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 and confidential information about many data subjects on behalf of the data controller.

After a review of the case, the Norwegian Data Protection Authority finds no basis for overriding the UFST's assessment that the supervision of the data processor Netcompany has taken place in accordance with the rules in Article 5, paragraph 1 of the Data Protection Regulation. 2, cf. subsection 1.

The Danish Data Protection Authority has thereby emphasized that UFST supervises Netcompany annually, and that the supervision includes an assessment of Netcompany's compliance with the data processing agreement.

The Danish Data Protection Authority has also emphasized that UFST has supervised Netcompany by obtaining an ISAE3000 declaration and an ISAE3402 declaration, that UFST has reviewed the declarations and followed up with some follow-up questions, and that UFST has then dealt with the answers.

[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] https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf