Supervision of the Ministry of Defence's Personnel Board's supervision of two data processors

Date: 15-12-2022

Decision

Public authorities

No criticism

Supervision / self-management case

Basic principles

Data processor

The Ministry of Defence's Personnel Board's supervision of two data processors did not give rise to criticism.

Journal number: 2021-421-0098

Summary

The Norwegian Data Protection Authority has carried out a written inspection of the Ministry of Defence's Personnel Board's inspection of two of the agency's data processors.

The Danish Data Protection Authority found no basis for overriding the Ministry of Defence's Personnel Board's assessment that the agency's supervision of the data processors Falck Healthcare A/S and Itadel had taken place in accordance with the data protection rules.

In the assessment, the Danish Data Protection Authority emphasized that the Ministry of Defence's Personnel Board had supervised the agency's data processor Falck Healthcare A/S by sending a request for a written status on matters covered by the data processing agreement, including some selected topics. The board had also considered the responses and assessed that they gave sufficient indication that Falch Healthcare A/S complies with the data processing agreement.

The Danish Data Protection Authority also emphasized that the Ministry of Defence's Personnel Board had supervised the agency's data processor Itadel by obtaining audit statements and requesting further documentation that Itadel had carried out appropriate supervision of their sub-data processors. The Ministry of Defence's Personnel Board had also agreed, in addition to the annual inspection and notification obligation in the event of any breaches, that Itadel actively informs the agency of current information security threats, vulnerabilities or incidents that may affect the agency's solution.

Decision

1. Written supervision of the Ministry of Defence's Personnel Board

The Ministry of Defence's Personnel Board (hereafter FPS) was among the authorities that the Danish Data Protection Authority had selected in autumn 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 FPS' inspection of data processors.

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

FPS appeared on 1 February 2022 with a list of the agency's data processors.

Based on the list, the Danish Data Protection Authority chose to check FPS' supervision of the agency's data processors Falck Healthcare A/S (hereafter Falck Healthcare) and Gnosis Data Analytics PC (hereafter Gnosis).

However, FPS stated by telephone on February 28, 2022 that FPS ceased cooperation with Gnosis in 2020.

On this basis, the Danish Data Protection Authority chose to carry out an inspection of FPS' supervision of the agency's data processor Itadel instead of Gnosis.

The Danish Data Protection Authority requested FPS to provide information on:

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

whether the agency has supervised the selected data processors, and

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

As far as Falck Healthcare is concerned, FPS sent a statement on the matter on 17 March 2022.

On 31 March 2022, FPS sent a statement in the case concerning Itadel.

2. Decision

After a review of the case, the Danish Data Protection Authority finds no basis for overriding FPS's assessment that the agency's supervision of the data processors Falck Healthcare and Itadel 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

FPS has stated that FPS has a supervision plan for both Falck Healthcare and Itadel. The supervision plan is documented in an excel sheet, supplemented by FPS' internal process description on supervision of data processors. The background for the supervision plan is a categorization of data processors according to the method described in the Norwegian Data Protection Authority's guidance on supervision of data processors. The frequency is basically one annual inspection, this also applies to Falck Healthcare and Itadel. This starting point is waived if the risk associated with a given data processor justifies an adjustment of the frequency.

3.1. Falck Healthcare

It appears from the case that Falck Healthcare processes personal data as a data processor for FPS in connection with specialist medical reports. In this connection, Falck Healthcare processes first and last name, social security number, address, information about the type of specialist doctor's report to be obtained, information about pending cases at the Health Board, date and time of consultation and any information about non-attendance from consultation.

FPS has stated that Falck Healthcare is supervised according to the so-called concept 3, cf. the Danish Data Protection Authority's guidance on supervision of data processors, including the points in the data processor agreement which are deemed to be most significant.

In this connection, FPS has stated that the agency has carried out these inspections with Falck Healthcare by sending a request for a written status on matters covered by the data processing agreement. The request emphasizes that this status must, as a minimum, describe how selected topics in the data processing agreement are complied with. During the inspection of Falck Healthcare, the selected subjects were:

Organization of the work with Information Security in general

Access control

Logging of access to personal data

Ensuring appropriate encryption when transmitting personal data

What breaches the data processor has had that are relevant to FPS

Regarding the follow-up to the inspection carried out, FPS has stated that Falck Healthcare has been informed that FPS had

no comments on their response, since FPS assessed that Falck Healthcare's response gave sufficient indication that Falck Healthcare complies with the data processing agreement. The head of the legal department in FPS, which is the contract owner of the agreement with Falck Healthcare, has been informed of the outcome of the inspection.

3.2. Ita nobility

It appears from the case that Itadel processes personal data as a data processor for FPS in connection with Novax Session Terminal access. In this connection, Itadel processes information about racial or ethnic background, religious beliefs, political affiliation/belief, health conditions, e.g. through diary notes, sexual orientation as well as information about purely private matters, significant social problems and criminal matters, social security number and information from the CPR register, name, address, contact information, job title, social problems, sick days, work-related matters, family matters and other private matters.

It also appears from the case that the processing consists of registration, processing, archiving, persistence and passing on of health data to the relevant and necessary extent.

FPS has stated that Itadel is supervised according to the so-called concept 6, cf. the Danish Data Protection Authority's guidance on supervision of data processors.

In addition to the annual supervision and notification obligation in case of any data breaches, it is agreed that Itadel actively informs FPS about current information security threats, vulnerabilities or incidents that may affect FPS's solution. FPS has learned that Itadel informs FPS about such matters several times a year, after which FPS's information security staff enters into a dialogue with Itadel about how the matter should be handled.

FPS has also stated that FPS has supervised Itadel by carrying out a documented inspection itself. The most recent inspections were carried out before the publication of the Danish Data Protection Authority's guidance on supervision of data processors, but the inspection method corresponds to concept 6. Specifically, FPS obtained an ISAE 3000 audit statement, which aims to document Itadel's general compliance with the regulation, as well as an ISAE 3402 audit statement, which documents Itadel's IT controls. Both audit statements were prepared by PWC in the year before FPS' inspection. In addition, Itadel was requested to provide additional documentation that they had properly supervised their sub-processors. A virtual meeting was also held where FPS asked in-depth questions based on the material received.

Regarding the follow-up to the inspection carried out, FPS has stated that the material sent, together with Itadel's oral and

written answers to the follow-up questions, was satisfactory. Itadel was informed by telephone that the inspection did not give rise to comments. The head of FPS, who is the contract owner of the agreement with Itadel, was verbally informed about the outcome of the inspection.

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.

It further appears from the guidance that supervision based on a documented supervision of the data processor carried out by the data controller himself (concept 6) or an independent third party (concept 5) are ways 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.

It also appears from the guidance that an inspection, where the data processor annually gives the data controller a written status of matters covered by the data processor agreement (concept 3), is a way in which the data controller can carry out appropriate supervision when the data processor's processing of personal data on behalf of the data controller is less risky.

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

The Danish Data Protection Authority has hereby emphasized that FPS has supervised Falck Healthcare by sending a request for a written status on matters covered by the data processing agreement, including some selected topics, and that FPS has considered the answers and assessed that they gave sufficient indication that Falck Healthcare complies with the data processing agreement.

The Danish Data Protection Authority has also emphasized that FPS has supervised Itadel by obtaining an ISAE3000 audit statement and an ISAE3402 audit statement, that FPS also requested Itadel to send additional documentation that they had conducted appropriate supervision of their sub-data processors, and that FPS in addition to the annual inspection and notification obligation in the event of any breach, has agreed with Itadel that the data processor actively informs FPS of current information security threats, vulnerabilities or incidents that may affect FPS's solution.

The Danish Data Protection Authority thus finds no reason to override FPS' assessment that the agency's supervision of Falck Healthcare and Itadel 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] https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf