Supervision of notification of breaches of personal data security: AROS Privathospital Partnerselskab

Date: 08-12-2020

Decision

Public authorities

In the supervision of AROS Privathospital Partnerselskab, the Danish Data Protection Agency concludes that AROS Privathospital Partnerselskab's processing of personal data is generally organized and carried out in accordance with the rules in the Data Protection Ordinance.

Journal number: 2019-41-0037

Summary

In November 2020, the Danish Data Protection Agency completed 15 planned inspections to shed light on the data controllers' ability to make the relevant reports of breaches of personal data security. In general, it has been gratifying to be able to state that all the data controllers examined have focused on the task, where in the respective organizations there was the necessary knowledge and routine, so that security incidents were intercepted and reported.

Criticism has been expressed in two of the cases: Both incidents were notifiable breaches of personal data security, which were only classified as security incidents. The specific assessment of whether there was a processing of information on natural persons was not made correctly by the actor in question.

AROS Privathospital Partnerselskab was among the private companies that the Danish Data Protection Agency had chosen in the spring of 2019 to supervise in accordance with the Data Protection Ordinance [1] and the Data Protection Act [2].

The Data Inspectorate's inspection was a written inspection, which focused in particular on whether AROS Privathospital Partnerselskab reports breaches of personal data security in accordance with Article 33 (1) of the Data Protection Regulation. And whether the private hospital meets the requirement to document all breaches of personal data security, cf. Article 33, para. 5.

AROS Privathospital Partnerselskab has also, in connection with the supervision, at the request of the Danish Data Protection Agency, generally reported on the private hospital's training of employees - in relation to dealing with breaches of personal data security - in order for the private hospital to comply with Article 33 of the Data Protection Regulation.

The Danish Data Protection Agency's supervision was notified to AROS Privathospital Partnerselskab by letter dated 11 March

2019, and the private hospital was requested on the same occasion to e.g. to answer a series of questions.

By letter dated 13 March 2019, AROS Privathospital Partnerselskab sent a statement in which the private hospital in connection with the answers to the Data Inspectorate's questions stated that the private hospital has no registered breaches of personal data security in the period from 25 May 2018 to 8 March 2019. AROS Privathospital The partner company's response was also accompanied by two documents on the hospital's handling of personal data, which the private hospital uses to comply with Article 33 of the Data Protection Regulation.

Decision

Considering that AROS Privathospital Partnerselskab did not register a breach of personal data security during the period in question, and as the Authority has not found any indications that this should have happened, the Danish Data Protection Agency has found that the Private Hospital has taken the necessary measures to be able to comply with the requirements of Article 33 (1) of the Data Protection Regulation 1, and thereby ensure that breaches of personal data security are detected in the organization and registered, so that these are always assessed with a view to whether the breach must be reported to the Danish Data Protection Agency.

On the basis of the information available, the Danish Data Protection Agency has assessed that AROS Privathospital Partnerselskab as a whole has complied with the requirements of Article 33 (1) of the Data Protection Regulation. 5.

In addition, the Danish Data Protection Agency's assessment is that AROS Privathospital Partnerselskab has carried out appropriate training activities, e.g. in order to be able to support the identification and management of breaches of personal data security.

Below is a more detailed review of the information that has emerged in connection with the audit and a justification for the Danish Data Protection Agency's decision.

2. Notification of breaches of personal data security

A breach of personal data security is defined in Article 4 (12) of the Data Protection Regulation as a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise treated.

It also follows from Article 33 (1) of the Data Protection Regulation (1) that in the event of a breach of personal data security, the controller shall, without undue delay and if possible within 72 hours after the controller has become aware of the breach of

personal data security, notify the supervisory authority competent in accordance with Article 55, unless the breach of personal data security is unlikely to involve a risk to the rights or freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it must be accompanied by a reason for the delay.

In the private hospital's statement of 13 March 2019 to the Danish Data Protection Agency, AROS Privathospital Partnerselskab stated that in the period from 25 May 2018 to 8 March 2019, no incidents were registered that were categorized as actual breaches of personal data security, cf. Article of the Data Protection Regulation 4, No. 12.

The Danish Data Protection Agency has not found any indications that there have been incidents that should have been reported, and has therefore found during the audit that AROS Privathospital Partnerselskab has complied with the requirement that all relevant breaches of personal data security have been reported to the Danish Data Protection Agency, cf. Article 33 (1) of the Data Protection Regulation 1.

Overall, the Danish Data Protection Agency has therefore not found grounds to conclude that AROS Privathospital Partnerselskab has registered information security incidents, including breaches of personal data security, which should have been reported to the Danish Data Protection Agency, but which have not occurred.

Documentation of breaches of personal data security

According to Article 33 (1) of the Data Protection Regulation 5, the data controller shall document all breaches of personal data security, including the facts of the breach of personal data security, its effects and the remedial measures taken. This documentation must be able to enable the supervisory authority (Datatilsynet) to check that the provision has been complied with.

It is noted that no specific formal requirements are set for the documentation, and the data controller can therefore decide for himself how the information is to be collected and how it is to be presented. However, the documentation must in all cases contain a number of information, cf. the wording of the provision above. The Danish Data Protection Agency's guidelines from February 2018 on handling breaches of personal data security state on page 27 that the requirements for documentation can be set out as follows:

Date and time of the breach

What happened in connection with the breach?

What is the cause of the fracture?

What (types) of personal information are covered by the breach?

What are the consequences of the breach for the affected persons?

What remedial action has been taken?

Whether - and if so how - has the Danish Data Protection Agency been notified? Why / Why not?

The data controller should thus document his reasons for all significant decisions made as a result of the breach. This applies not least if the data controller, after assessing the breach, has come to the conclusion that it should not be reported to the Danish Data Protection Agency.

In connection with the audit, AROS Privathospital Partnerselskab has stated that the private hospital has not experienced a breach of personal data security. The private hospital has thus not been in possession of material that could document the handling of violations. The Danish Data Protection Agency has not found any indications of incidents that should have been listed.

On the basis of the submitted documentation, it is the Data Inspectorate's assessment that AROS Privathospital Partnerselskab has overall complied with the requirements of Article 33 (1) of the Data Protection Regulation. 5.

4. Training of employees

It is clear from Article 32 (1) of the Data Protection Regulation 1, that the data controller must implement appropriate technical and organizational measures to ensure an appropriate level of security.

Among other things, is required that the data controller must ensure that all employees in the organization are, to the extent necessary, aware of any internal procedures for handling breaches of personal data security, that certain relevant employees can identify and assess breaches of personal data security, in addition it is a necessity for that the organization as a whole is otherwise able to support the obligation to make reports, etc. pursuant to Article 33 of the Data Protection Regulation.

The Danish Data Protection Agency has noted that AROS Privathospital Partnerselskab has stated that two activities have been held with a view to training all hospital employees in being able to identify and handle breaches of personal data security.

The Danish Data Protection Agency has not had the opportunity to take a specific position on whether all relevant employees have completed the training activities in question, and the Authority is not familiar with the training material used. .a. in order to be able to support the identification and management of breaches of personal data security. Depending on the circumstances, in particular that there are no indications of breach and what is otherwise elucidated in the case, the Authority has found the

level of information appropriate

5. Summary

Considering that AROS Privathospital Partnerselskab during the period did not register breaches of personal data security, and as the Authority has not found any indications that this should have happened, the Danish Data Protection Agency has found that the Private Hospital has taken the necessary measures to comply with the requirements of Article 33 (1) of the Data Protection Regulation 1, and thereby ensure that breaches of personal data security are detected in the organization and registered, so that these are always assessed with a view to whether the breach must be reported to the Danish Data Protection Agency.

On the basis of the conciliation, the Danish Data Protection Agency has assessed that AROS Privathospital Partnerselskab as a whole has complied with the requirements of Article 33 (1) of the Data Protection Regulation. 5.

In addition, the Danish Data Protection Agency's assessment is that AROS Privathospital Partnerselskab has carried out appropriate training activities, e.g. in order to be able to support the identification and management of breaches of personal data security.

The Danish Data Protection Agency hereby considers the case closed and does not take any further action.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation)

[2] Act No. 502 of 23 May 2018 on additional provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (Data Protection Act)