

Supervision of reports of breaches of personal data security: The Danish Agency for Patient Complaints

Date: 08-12-2020

Decision

Public authorities

In the supervision of the Danish Agency for Patient Complaints, the Danish Data Protection Agency concludes that the Danish Agency for Patient Complaints' processing of personal data is generally organized and carried out in accordance with the rules in the Data Protection Ordinance.

Journal number: 2019-421-0030

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.

The Danish Agency for Patient Complaints was among the public authorities 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 the Danish Agency for Patient Complaints reports breaches of personal data security in accordance with Article 33 (1) of the Data Protection Regulation. And whether the Agency fulfills the requirement to document all breaches of personal data security, cf. Article 33, para. 5.

The Danish Agency for Patient Complaints has also, in connection with the audit, at the request of the Danish Data Protection Agency, generally reported on the agency's training of employees - in relation to handling breaches of personal data security - in order for the agency to comply with Article 33 of the Data Protection Ordinance.

The Danish Data Protection Agency's supervision was notified to the Danish Agency for Patient Complaints by letter dated 11

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

By letter dated 14 March 2019, the Danish Agency for Patient Complaints sent a statement in which the Agency, in connection with the answers to the Danish Data Protection Agency's questions, sent documentation (in the form of several documents) that highlights all registered information security incidents, including all registered breaches of personal data security. in the period from 25 May 2018 to and including 8 March 2019. The Danish Agency for Patient Complaints' response was also accompanied by a number of other documents, including guidelines and a process description, which the Agency uses to comply with Article 33 of the Data Protection Regulation.

Decision

Following the audit of the Danish Agency for Patient Complaints, the Danish Data Protection Agency finds reason to conclude that the Danish Agency for Patient Complaints' processing of personal data is generally organized and carried out in accordance with the rules in Article 33 of the Data Protection Ordinance.

In the opinion of the Danish Data Protection Agency, the Danish Agency for Patient Complaints has thus implemented the measures necessary 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.

Furthermore, the Danish Data Protection Agency finds that the Danish Agency for Patient Complaints has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

In addition, the Danish Data Protection Agency's assessment is that the Danish Agency for Patient Complaints 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 Agency's statement of 14 March 2019 to the Danish Data Protection Agency, the Danish Agency for Patient Complaints stated that in the period from 25 May 2018 to and including 8 March 2019, a total of 81 information security incidents have been registered with the Agency. According to the Danish Agency for Patient Complaints, 5 of these information security incidents are "pure" information security incidents, which in the Agency's assessment cannot be described as breaches of personal data security, and thus only 76 incidents that the Danish Agency for Patient Complaints has categorized as actual breaches of personal data security. 4, no. 12. Out of the 76 breaches, the Danish Agency for Patient Complaints has reported the 33 to the Danish Data Protection Agency, and in 43 remaining cases the Agency has assessed that there was no obligation to report the breach to the Danish Data Protection Agency.

During the audit, the Danish Data Protection Agency has taken a position on whether the Danish Agency for Patient Complaints has complied with the requirement that all relevant breaches of personal data security have been reported to the Danish Data Protection Agency, cf. 1.

With regard to the 76 incidents, the Danish Data Protection Agency has received 33 of them as reports of breaches of personal data security. For the 43 incidents which have been categorized by the Danish Agency for Patient Complaints as breaches of personal data security, but which have not been reported to the Danish Data Protection Agency, the Authority may agree with the Agency's assessment that the incidents in question can be characterized as breaches of personal data security. No. 12, but that these are not covered by the obligation to make a notification. In this connection, the Danish Data Protection Agency has assessed that it must be described as unlikely that the violations in question entail a risk to the rights and freedoms of natural persons, cf. Article 33 (1). 1.

Overall, the Danish Data Protection Agency has therefore not found grounds to conclude that the Danish Agency for Patient Complaints 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 been.

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.

The 76 breaches of personal data security, about which the Danish Agency for Patient Complaints has submitted material in connection with the inspection, are divided into two separate lists (incident logs). One list lists 48 breaches, of which 22 have been reported to the Danish Data Protection Agency, and the other list contains information on 28 breaches, of which 11 cases have been reported.

After reviewing the Danish Agency for Patient Complaints' own documentation for the 33 breaches of personal data security, which the board has reported to the Danish Data Protection Agency, the Authority can state that the board has described the

facts of the breach and stated a reason why the breach was reported to The Data Inspectorate.

It is - after reviewing all the material in question - the Data Inspectorate's assessment that the Agency as a whole has provided the required documentation.

Against this background, it is the Danish Data Protection Agency's assessment that the Danish Agency for Patient Complaints has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

The Danish Data Protection Agency has also reviewed the Danish Agency for Patient Complaints' own documentation for the 43 breaches of personal safety, which have not been reported to the Danish Data Protection Agency. In this connection, the Authority can state that the Agency has described the actual circumstances of the breach and stated a reason why the breach was not reported to the Danish Data Protection Agency. The Danish Data Protection Agency has assessed that the scope of the stated documentation has been sufficient for the Authority to be able to conclude that it must be described as unlikely that the violations in question entail a risk to the rights and freedoms of natural persons, cf. Article 33 (1) of the Regulation. 1.

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 the Danish Agency for Patient Complaints has prepared instructions and carried out a number of activities with a view to training employees in data protection, including with a view to employees being able to identify and possibly handle breaches of personal data security.

Notwithstanding that 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 notwithstanding that the Authority is not aware of the full content of the training material, it is the Authority's assessment. appropriate educational activities i.a. in order to be able to support the identification and management of breaches of personal data security.

5. Summary

Following the audit of the Danish Agency for Patient Complaints, the Danish Data Protection Agency finds reason to conclude that the Danish Agency for Patient Complaints' processing of personal data is generally organized and carried out in accordance with the rules in Article 33 of the Data Protection Ordinance.

In the opinion of the Danish Data Protection Agency, the Danish Agency for Patient Complaints has thus implemented the measures necessary 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.

Furthermore, the Danish Data Protection Agency finds that the Danish Agency for Patient Complaints has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

In addition, the Danish Data Protection Agency's assessment is that the Danish Agency for Patient Complaints 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)