Supervision of reports of breaches of personal data security: Køge Municipality

Date: 08-12-2020

Decision

Public authorities

In the audit of Køge Municipality, the Danish Data Protection Agency concludes that there is a basis for expressing criticism. In a single case, Køge Municipality has not complied with the requirement that all processing of personal data is organized and carried out in accordance with the rules in the Data Protection Ordinance.

Journal number: 2019-423-0207

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.

Køge Municipality 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 Køge Municipality reports breaches of personal data security in accordance with Article 33 (1) of the Data Protection Regulation. 1, and whether the municipality meets the requirement to document all breaches of personal data security, cf. Article 33, para. 5.

In connection with the inspection, Køge Municipality has also, at the request of the Danish Data Protection Agency, generally reported on the municipality's training of employees - in relation to handling breaches of personal data security - in order for the municipality to comply with Article 33 of the Data Protection Ordinance.

The Data Inspectorate's inspection was notified to Køge Municipality by letter dated 11 March 2019, and the municipality was requested on the same occasion to e.g. to answer a series of questions.

By letter dated 14 March 2019, Køge Municipality sent a statement in which the municipality, in connection with the answers to the Danish Data Protection Agency's questions, sent documentation (in the form of several documents) that sheds light on all registered information security incidents, including all registered breaches of personal data security. the period from 25 May 2018 to and including 8 March 2019. Køge Municipality's response was also attached to a number of other documents, including the municipality's information security policy, pamphlets and procedure descriptions, which the municipality uses to comply with Article 33 of the Data Protection Regulation.

Decision

Following the audit of Køge Municipality, the Danish Data Protection Agency finds reason to conclude in summary that there is a basis for expressing criticism that Køge Municipality in a single case has not complied with the requirement that all processing of personal data is organized and performed in accordance with the rules of Article 33 of the Data Protection Regulation.

In the remaining cases examined, it is the opinion of the Danish Data Protection Agency that Køge Municipality has 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 Køge Municipality has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

In addition, it is the Data Inspectorate's assessment that Køge Municipality has carried out appropriate educational activities, e.g. in order to be able to support the identification and management of breaches of personal data security.

It also appears from the case that Køge Municipality has initiated various activities with a view to educating and informing employees about data protection, including the handling 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 municipality's statement of 14 March 2019 to the Danish Data Protection Agency, Køge Municipality has stated that in the period from 25 May 2018 to and including 8 March 2019, a total of 31 information security incidents have been registered in the municipality. According to Køge Municipality, 10 of these information security incidents are "pure" information security incidents, which in the municipality's assessment can not be described as breaches of personal data security, and thus only 21 incidents that Køge Municipality has categorized as actual breaches of personal data security, cf. Article 4 of the Data Protection Regulation. no. 12. Out of the 21 breaches, Køge Municipality has reported the 11 to the Danish Data Protection Agency, two cases are considered reported to the Danish Data Protection Agency in connection with complaints processed by the Danish Data Protection Agency and in the 8 remaining cases the municipality 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 Køge Municipality 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 Ordinance. 1.

With regard to the 10 incidents which have been categorized by Køge Municipality as “pure” information security incidents, the Danish Data Protection Agency has assessed these and concluded that one of these incidents should have been registered as a breach of personal data security. This one incident has been registered on 18 June 2018 and relates to a fracture that occurred in Køge Municipality's dental care under the Children and Education Administration. The municipality has stated in the incident description from the same date that due to storage of information on a public drive without access control, there has been free access to patient information in the form of dental data, including name, cpr. information, patient data and X-rays, and that the date and time of the fracture are unknown. The municipality has also assessed that it is unlikely that the breach entails a risk to the data subjects and their rights, on the grounds that there is minimal risk of knowing the exact path to

the X-ray file in which the said personal information was stored and therefore, is the breach has not been reported. It does not appear from the submitted documentation how many people are affected by the breach.

Based on the information provided by Køge Municipality in the incident description, the Danish Data Protection Agency has based the following:

that Køge Municipality is data responsible for the processing of the information at the dental care

that there has been unintentional potential access to personal information, including name, social security number, patient data and X-rays, which were placed in a folder on the municipality's administrative network, as no access restriction had been made to the contents of the folder

that access to the files has not been checked by logging or similar measure.

that no evidence has been substantiated that the access can not be used by other employees in the municipality with access to the network

that it is not clear how many people are affected by the breach

that the date and time of the breach are not known, and thus it is not known how long the breach has lasted

that it is not clear whether it has been assessed, whether it has been necessary to inform those affected

Against this background, the Danish Data Protection Agency is of the opinion that this is a breach of personal data security, cf. Article 4, no. 12 of the Data Protection Regulation, as there has been unintentional access to the personal data in question that was processed during storage. Considering that Køge Municipality has stated that there has been no access restriction to the path on the network, and since the municipality has not been able to prove that this access has not been used (eg by documenting logs), it can not be considered unlikely that there has been a risk to the rights of data subjects. The breach must therefore appear in part in Article 33 (1). 5 list and should have been notified to the Danish Data Protection Agency, cf. Article 33 (1) of the Data Protection Regulation. 1.

With regard to the 9 other “pure” information security incidents, the Danish Data Protection Agency has not found grounds to override the municipality's assessment that the incidents in question do not have the character of a breach of personal data security, cf. Article 4, no. 12 of the Data Protection Regulation.

With regard to the remaining 21 incidents, the Danish Data Protection Agency has received 11 of them as reports of breaches of personal data security and two as complaints. Due to lack of documentation, the Authority has found reason to - in addition

to the submitted material - review the two complaints about Køge Municipality, which the Data Inspectorate has received, to assess whether the municipality should have reported these. According to what was stated in the cases, there are 2 matters in which the municipality has deliberately published the information, and has intended to have a legal basis for this. The Danish Data Protection Agency agrees, given that the two cases do not violate personal data security, cf. Article 4, no. 12 of the Data Protection Scheme, and therefore - correctly - have not been notified to the Authority, cf.

For the eight incidents that are categorized by Køge Municipality as breaches of personal data security, but which have not been reported to the Danish Data Protection Agency, the Authority can agree with the municipality's assessment that the incidents in question can be characterized as breaches of personal data security. 12, but that these are not subject to 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 finds that Køge Municipality has generally implemented the measures necessary to comply with the requirements of Article 33 (1) of the Data Protection Ordinance. 1, but the Authority finds it criticisable that no notification has been made to the Authority of the incident in question registered on 18 June 2018.

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 21 breaches of personal data security, about which Køge Municipality has submitted material in connection with the inspection, appear from a separate list. This list lists the 11 breaches that have been reported to the Danish Data Protection Agency and the 10 breaches where no notification has taken place.

After reviewing Køge Municipality's own documentation for the 11 breaches of personal data security that the municipality has reported to the Danish Data Protection Agency, the Authority can in this connection state that the municipality 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 municipality as a whole has provided the required documentation.

Against this background, it is the Danish Data Protection Agency's assessment that Køge Municipality as a whole has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

The Danish Data Protection Agency has also reviewed Køge Municipality's own documentation for the 8 breaches of personal security, which have not been reported to the Danish Data Protection Agency. In this connection, the Authority can state that the municipality 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 Køge Municipality has prepared pamphlets and carried out a number of activities with a view to educating 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, the Authority's assessment is that Køge Municipality has completed 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 Køge Municipality, the Danish Data Protection Agency finds reason to conclude in summary that there is a basis for expressing criticism that Køge Municipality in a single case has not complied with the requirement that all processing of personal data is organized and performed in accordance with the rules of Article 33 of the Data Protection Regulation.

In the opinion of the Danish Data Protection Agency, Køge Municipality has thus generally 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 Køge Municipality has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

In addition, it is the Data Inspectorate's assessment that Køge Municipality has carried out appropriate educational activities, e.g. in order to be able to support the identification and management of breaches of personal data security.

6. Completion

The Danish Data Protection Agency notes that the Authority's decision cannot be appealed to another administrative authority, cf. section 30 of the Data Protection Act.

The Danish Data Protection Agency's decision may, however, be brought before the courts, cf. section 63 of the Constitution.

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)