Supervision of reporting breaches of personal data security: Esbjerg Municipality

Date: 08-12-2020

Decision

Public authorities

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

Journal number: 2019-423-0203

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.

Esbjerg 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 Esbjerg 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 audit, Esbjerg 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 - with a view to the municipality complying with Article 33 of the Data Protection Ordinance.

The Danish Data Protection Agency's supervision was notified to Esbjerg 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 12 March 2019, Esbjerg 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. Esbjerg Municipality's response was also attached to a number of other documents, including guidelines, process descriptions and teaching materials, which the municipality uses to comply with Article 33 of the Data Protection Regulation.

Decision

Following the supervision of Esbjerg Municipality, the Danish Data Protection Agency finds reason to conclude that Esbjerg Municipality's processing of personal data is generally organized and carried out in accordance with the rules in Article 33 of the Data Protection Regulation.

In the opinion of the Danish Data Protection Agency, Esbjerg Municipality 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 Esbjerg Municipality as a whole 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 Esbjerg 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 Esbjerg 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 data 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 12 March 2019 to the Danish Data Protection Agency, Esbjerg Municipality has stated that in the period from 25 May 2018 to and including 8 March 2019, a total of 60 information security incidents have been registered in the municipality. According to Esbjerg Municipality, 28 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 32 incidents that Esbjerg Municipality has categorized as actual breaches of personal data security, cf. Article 4 of the Data Protection Regulation. no. 12. Out of the 32 breaches, Esbjerg Municipality has reported the 24 to the Danish Data Protection Agency, and in 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 Esbjerg 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 28 incidents which are categorized by Esbjerg Municipality as “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 breaches of personal data security, cf. No. 12.

With regard to the remaining 32 incidents, the Danish Data Protection Agency has received 24 of these as reports of breaches of personal data security. For the 8 incidents that are categorized by Esbjerg 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, cf. 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 has therefore not found grounds to conclude that Esbjerg Municipality 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 32 breaches of personal data security, about which Esbjerg Municipality has submitted material in connection with the audit, are divided into two separate lists. One list lists the 24 breaches that have been reported to the Danish Data Protection Agency, and the other list provides information on the 8 breaches where no reporting has taken place.

After reviewing Esbjerg Municipality's own documentation for the 24 breaches of personal data security, which the municipality has reported to the Danish Data Protection Agency, the Authority can ascertain that the submitted documentation appears to be incomplete, as e.g. lacks a description of the facts of the individual breach, the effects and consequences of the breach as well as any remedial measures taken.

The Danish Data Protection Agency has therefore not been able to check, on the basis of the material submitted alone, whether Article 33 (1) of the Data Protection Regulation 5, has been complied with. As a consequence, the Danish Data Protection Agency has had to - in addition to the material submitted in this case - review some of the notification forms that the Danish Data Protection Agency has received from Esbjerg Municipality in order to assess whether the municipality at the time of the notifications had sufficiently elucidated and documented the breaches, and whether the municipality, on that basis after an assessment of the overall information in the possession of the Danish Data Protection Agency, has complied with the requirement for documentation, cf. Article 33 (1) of the Data Protection Ordinance. 5.

It is - after reviewing all the material in question - the Data Inspectorate's assessment that the municipality as a whole would have been able to provide the required documentation. In this connection, the Danish Data Protection Agency has assumed that the municipality - as a public authority - has kept a copy of the notifications, and that these could thus have been sent to the Danish Data Protection Agency upon renewed request.

On that basis, it is the Data Inspectorate's assessment that Esbjerg Municipality as a whole has complied with the requirements of Article 33 (1) of the Data Protection Ordinance. 5.

However, in continuation of the above - and not least in light of the Data Inspectorate's guidelines from February 2018 on handling breaches of personal data security - the Data Inspectorate must recommend to Esbjerg Municipality that the municipality in future be much more aware of the benefit of having a comprehensive structured overview of all breaches. on personal data security and any information security incidents. In the opinion of the Danish Data Protection Agency, such an overview could also contribute to Esbjerg Municipality becoming better at continuously analyzing and following up on the breaches of personal data security that the municipality has, which can prevent new breaches of personal data security. In addition, it could help reduce the effects of future breaches. In this connection, the Danish Data Protection Agency may mention that a similar measure appears in the information security standard ISO 27001, Annex A, section 16.1.6.

The Danish Data Protection Agency has also reviewed Esbjerg 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 specified documentation has been sufficient for the Authority to be able to conclude that it must be described as unlikely that the violations in question involve 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 Esbjerg Municipality has prepared guidelines 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, including the content of e.g. the e-learning course, it is the Authority's assessment that Esbjerg 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.

5. Summary

Following the supervision of Esbjerg Municipality, the Danish Data Protection Agency finds reason to conclude that Esbjerg Municipality's processing of personal data is generally organized and carried out in accordance with the rules in Article 33 of the Data Protection Regulation.

In the opinion of the Danish Data Protection Agency, Esbjerg Municipality 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 Esbjerg Municipality as a whole 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 Esbjerg 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.

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)