Supervision of reporting of breaches of personal data security: Aalborg University

Date: 08-12-2020

Decision

Public authorities

In the supervision of Aalborg University, the Danish Data Protection Agency concludes that Aalborg University's processing of personal data is generally organized and carried out in accordance with the rules in the Data Protection Ordinance. However, criticism is expressed that Aalborg University's documentation has not been sufficient in connection with security incidents involving the theft of IT equipment.

Journal number: 2019-421-0032

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.

Aalborg University 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 Aalborg University reports breaches of personal data security in accordance with Article 33 (1) of the Data Protection Regulation. And whether the university meets the requirement to document all breaches of personal data security, cf. Article 33, para. 5.

In connection with the supervision, Aalborg University has, at the request of the Danish Data Protection Agency, generally reported on the university's training of employees - in relation to handling breaches of personal data security - with a view to the university being able to comply with Article 33 of the Data Protection Regulation.

The Danish Data Protection Agency's audit was notified to Aalborg University by letter dated 11 March 2019, and the university

was requested on the same occasion to e.g. to answer a series of questions.

By letter dated 14 March 2019, Aalborg University sent a statement in which the university, 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. Aalborg University's response was also attached to a number of other documents, including the university's information security policy, procedure descriptions and templates, which the university uses to comply with Article 33 of the Data Protection Regulation.

Decision

Following the audit of Aalborg University, the Danish Data Protection Agency finds reason to conclude that Aalborg University's 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, Aalborg University has thus implemented the measures necessary to be able to comply with the requirements of Article 33 (1) of the Data Protection Ordinance. 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.

However, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Aalborg University's documentation in connection with the security incidents that involved the theft of IT equipment has not been sufficient, cf. Article 33 (1) of the Data Protection Ordinance. 5.

The Danish Data Protection Agency has emphasized here that it has not been possible for the Authority - based on the submitted documentation - to assess whether these are security incidents that should have been reported to the Danish Data Protection Agency, cf. Article 33 (1) of the Data Protection Regulation. 1, including what is missing in particular if information about natural persons was stored on the equipment.

In addition, however, the Danish Data Protection Agency finds that Aalborg University has otherwise - overall - 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 Aalborg University 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 Aalborg University 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.

Aalborg University has in the university's statement of 14 March 2019 to the Danish Data Protection Agency stated that in the period from 25 May 2018 to and including 8 March 2019, a total of 102 information security incidents have been registered at the university. According to Aalborg University, 75 of these information security incidents are "pure" information security incidents, which in the University's assessment cannot be described as breaches of personal data security, and thus only 27 incidents that Aalborg University has categorized as actual breaches of personal data security, cf. No. 12. Out of the 27 breaches, Aalborg University has reported the eight to the Danish Data Protection Agency, and in 19 remaining cases the university has assessed that there was no obligation to report the breach to the Danish Data Protection Agency. Aalborg University has also enclosed an overview that sheds light on 63 incidents that the university has characterized as IT operational incident breaches.

During the audit, the Danish Data Protection Agency has taken a position on whether Aalborg University 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 75 incidents which are categorized by Aalborg University as "pure" information security incidents, the Danish

Data Protection Agency has in the cases involving theft of a computer or a mobile phone assessed that it is unclear whether these information security incidents have the character of being breaches. on personal data security, and therefore should have been registered and handled as such.

With regard to the remaining information security incidents and the 63 IT operational incidents, the Danish Data Protection Agency has not found grounds to override the university's assessment that the incidents in question are not in the nature of breaches of personal data security, cf. Article 4 (12) of the Data Protection Regulation.

With regard to the remaining 27 incidents, the Danish Data Protection Agency has received eight of these as reports of breaches of personal data security. For the 19 incidents that are categorized by Aalborg University as breaches of personal data security, but which have not been reported to the Danish Data Protection Agency, the Authority may agree with the university'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 Aalborg University 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. The Danish Data Protection Authority must emphasize, however, that theft of computers and other equipment on which information about natural persons is stored is covered by the definition in Article 4, no. 12 of the Data Protection Scheme, , it can be stated that it is unlikely that there is a risk to the rights and freedoms of natural persons, cf. Article 33 (1). As information about natural persons is most often stored in e-mail, photos or other stored files as well as user information, the Data Inspectorate is of the opinion that when this is not the case, it must appear from the documentation for the assessment of the incident in question.

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 27 breaches of personal data security, about which Aalborg University has submitted material in connection with the audit, appear from a separate list. The list lists the eight breaches that have been reported to the Danish Data Protection Agency, and information is given about the 19 breaches where no reporting has taken place.

Regarding the information security incidents, which include theft of a computer or a mobile phone, the Danish Data Protection Agency is of the opinion that these incidents - if there was information about natural persons on the computers in question - should appear in Aalborg University's 33 para. 5 list with the result that it will be stated why the incident should not be reported. In that case, the Authority would have been able to check whether the notification obligation pursuant to Article 33 (1) of the Data Protection Regulation 1 has been complied with.

It is - after reviewing all the material in question - the Data Inspectorate's assessment that the university as a whole has provided the required documentation, despite the fact that the Data Inspectorate has not been able to check whether the mentioned information security incidents are actual breaches of personal data security.

Against this background, it is the Data Inspectorate's assessment that Aalborg University 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 Aalborg University's own documentation for the 19 breaches of personal security, which have not been reported to the Danish Data Protection Agency. In this connection, the Authority can state that the university 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 Aalborg University has prepared guidelines for personal data 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 Aalborg University 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 audit of Aalborg University, the Danish Data Protection Agency finds reason to conclude that Aalborg University's 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, Aalborg University has thus implemented the measures necessary to be able to comply with the requirements of Article 33 (1) of the Data Protection Ordinance. 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.

However, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Aalborg University's documentation in connection with the security incidents that involved the theft of IT equipment has not been sufficient, cf. Article 33 (1) of the Data Protection Ordinance. 5.

The Danish Data Protection Agency has emphasized here that it has not been possible for the Authority - based on the submitted documentation - to assess whether these are security incidents that should have been reported to the Danish Data Protection Agency, cf. Article 33 (1) of the Data Protection Regulation. 1, including what is missing in particular if information about natural persons was stored on the equipment.

In addition, however, the Danish Data Protection Agency finds that Aalborg University has otherwise - overall - 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 Aalborg University 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)