Criticism of Aalborg University for lack of testing and insufficient control of user access

Date: 10-02-2023

Decision

Public authorities

Criticism

Reported breach of personal data security

Access control

Notification of breach of personal data security

Treatment safety

The Danish Data Protection Authority has made a decision in a case about Aalborg University, where students, employees and guest employees had access to personal data about the university's employees in a system.

Journal number: 2022-442-19476

Summary

The Danish Data Protection Authority has made a decision in a case where Aalborg University has reported a breach of personal data security.

Aalborg University established that for several years – probably since 2020 and until August 2022 – it had been possible for anyone with an AAU user profile (students, employees and guest employees) to access non-sensitive information about the university's employees in a system. Thus, the system had not had the necessary access restriction, as it is only IT employees at the university who need to use the system in their daily work.

In the case in question, Aalborg University stated that in connection with the migration to a new server and the rewriting of code in the system in the summer of 2020, human error most likely occurred, as no testing of access control in the system was subsequently carried out. In this connection, Aalborg University has stated that the university's guidelines have not been followed.

In its decision, the Danish Data Protection Authority emphasized that it is a prerequisite that tests are carried out after a change or update of a system to ensure that the established security requirements in a system continue to be implemented after the change or update. In addition, the Danish Data Protection Authority has emphasized that unauthorized persons have

had access to the system for several years, and that there has therefore not been sufficient ongoing control of user access to the system.

Decision

The Danish Data Protection Authority hereby returns to the case where Aalborg University reported a breach of personal data security to the Danish Data Protection Authority on 5 August 2022. The report has the following reference number: 5f79a4018d799ef0ca0082ef55449e0afc62609f.

1. Decision

After a review of the case, the Data Protection Authority finds that there is a basis for expressing criticism that Aalborg University's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

On 5 August 2022, Aalborg University reported a breach of personal data security to the Norwegian Data Protection Authority. It appears from the notification that for an unknown period until 3 August 2022 it has been possible for everyone with an AAU user profile (students, employees and guest employees) to log on to the IT system Webmanageren. The system has thus not had the necessary access restriction, as it is only IT employees who need to use the program in their daily work.

Aalborg University has informed the case that the IT system Webmanageren contains information about university employees, and that the vast majority of information has already been published on Aalborg University's website or internally in Outlook or Aalborg University's intranet, where all employees have access. In addition, the system contains technical information about e.g. the employee profile's creation, last login and changes.

It appears from the case that it is not possible for Aalborg University to clarify with certainty whether it is a technical or human error that is the cause of the incident.

Aalborg University has further stated that in connection with the migration to a new server and the rewriting of code in the Webmanager system in the summer of 2020, a human error has most likely occurred, as access control testing in the Webmanager system was not subsequently carried out. In this connection, Aalborg University has stated that Aalborg University's guidelines have not been followed.

Aalborg University has informed the case that the duration of the incident is unknown, but that it was probably from December 2020 until Aalborg University discovered the error on 3 August 2022. It also appears from the case that Aalborg University, on the basis of log- information from May 2019 has established that a search was made in the Webmanager system for the first time in February 2020 by an employee who is not an IT employee. In this connection, Aalborg University has stated that they have established that searches have been carried out on 7 people in the Webmanager system by employees at Aalborg University who are not IT employees.

It also appears from the case that there is a procedure description that was last updated on 26 August 2021, where it appears that access restrictions were set up during implementation, so that only IT employees had access to the program.

Aalborg University has also stated that they have not had occasion to check that the access restrictions had disappeared, as it has previously been documented that access restrictions had been configured on the Webmanager system.

Aalborg University has informed the matter that 29 minutes after the incident was discovered, all access to the Webmanager system was shut down to remedy the error. The access restriction was secured and tested before the access was opened again. It was thus ensured that only authorized employees have access.

It also appears from the case that Aalborg University's IT department has fixed procedures for technical setup, testing and use of access restrictions when implementing new software, and that the IT employees are instructed in these procedures.

The Danish Data Protection Authority has asked Aalborg University to send dated copies of the procedure descriptions referred to in order to process the case. Aalborg University has then forwarded extracts from the university's policy for information security as well as a security handbook, where the requirements for access control are stated. The Norwegian Data Protection Authority can ascertain that the detailed procedures for, among other things, test of access restriction, however, does not appear in the submitted material.

Aalborg University has also stated that the Webmanager system is not known or immediately accessible to anyone other than IT employees, as it will require knowledge of a technical path to the program. In addition, the user must log in with their AAU user.

It also appears from the case that Aalborg University is reviewing their procedures with a view to assessing whether stricter measures can be taken to avoid similar cases in the future.

3. Reason for the Data Protection Authority's decision

On the basis of information provided by Aalborg University on 5 August and 13 December 2022, the Data Protection Authority assumes that for an unknown period until 3 August 2022 it has been possible for everyone with an AAU user profile (students, employees and guest employees) to log on to the IT system Webmanageren and access information about Aalborg University's employees.

On this basis, the Danish Data Protection Authority assumes that there has been unauthorized access to personal data, which is why the Danish Data Protection Authority finds that there has been a breach of personal data security, cf. Article 4, No. 12 of the Data Protection Regulation.

3.1. Article 32 of the Data Protection Regulation

It follows from the data protection regulation, article 32, subsection 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the data controller's processing of personal data.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects against these risks.

The Danish Data Protection Authority is of the opinion that the requirement cf. Article 32 for adequate security will normally mean that when migrating to a new server and rewriting code in a system that processes personal data, the changes must be made according to established procedures, whereby the possible consequences of the changes are considered. The requirement will also entail that tests must be planned that can verify that the established security requirements, including access restrictions, are still met after the changes have been implemented.

In addition, the Danish Data Protection Authority is of the opinion that the requirement for adequate security will normally entail that the data controller continuously checks whether user access to systems with personal data is limited to those users who have a legitimate need to access the information in the system.

In this connection, the Danish Data Protection Authority must note that rights management in systems with personal data must prevent unauthorized access to personal data as well as unauthorized changes or loss of personal data in the system in cases where users have access to change or delete information.

Based on the above background, the Danish Data Protection Authority finds that Aalborg University - by not having carried out the necessary tests after changes to the system and not having carried out sufficient ongoing control of user access - has not

taken appropriate organizational and technical measures to ensure a level of security that suits the risks involved in Aalborg University's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

After a review of the case, the Data Protection Authority finds that there is a basis for expressing criticism that Aalborg University's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

When choosing a response, the Norwegian Data Protection Authority emphasized that it is a prerequisite to ensure that the established security requirements in a system are still implemented after a change or update thereof, that tests are carried out in connection with such changes or updates.

The Danish Data Protection Authority has further emphasized that unauthorized persons have had access to the Webmanager system for several years – probably since 2020 – and that there has therefore not been sufficient ongoing control of user access to the system.

The Data Protection Authority has noted that Aalborg University will review their procedures with a view to assessing whether stricter measures can be taken to avoid similar cases in the future.

3.2. Summary

On the basis of the above, the Danish Data Protection Authority finds that there is a basis for expressing criticism that Aalborg University's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).