Supervision of Køge Municipality's rights management in Aula

Date: 18-01-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Access control

Treatment safety

Journal number: 2021-423-0239

Summary

Køge Municipality was among the selected municipalities that the Data Protection Authority supervised in the summer of 2021 in accordance with the data protection rules.

The inspection focused on Køge Municipality's way of administering access rights in the area of children and young people, including especially the school area. In this connection, the Data Protection Authority investigated Køge Municipality's rights management in Aula.

The Danish Data Protection Authority found that Køge Municipality's control of users' rights in Aula was not in accordance with the rules on processing security.

The Danish Data Protection Authority emphasized that Køge Municipality had not had systematic checks and that the municipality had not carried out checks on users other than employees' access to Aula.

Against this background, the Danish Data Protection Authority criticized Køge Municipality.

1. Written supervision of Køge Municipality's processing of personal data

Køge Municipality was among the authorities that the Data Protection Authority had selected in the summer of 2021 to supervise according to the Data Protection Regulation[1] and the Data Protection Act[2].

The Danish Data Protection Authority's inspection was a written inspection which focused on Køge Municipality's way of administering access rights in the area of children and young people, including especially the school area, cf. Article 32 of the Data Protection Regulation.

By letter of 9 June 2021, the Data Protection Authority notified the supervisory authority of Køge Municipality. In this connection, the Danish Data Protection Authority requested to be sent a list of systems in the municipality's school area, in which information about natural persons is processed.

Køge Municipality issued a statement on the matter on 30 June 2021.

On the basis of the response, the Data Protection Authority chose to carry out further checks of Køge Municipality's rights management in Aula.

On 11 August 2021, the Danish Data Protection Authority requested Køge Municipality to explain how the municipality ensures that users' rights in Aula reflect rights restrictions in underlying systems. On that basis, the municipality sent a supplementary statement in the matter on 1 September 2021.

2. The Data Protection Authority's decision

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

Below follows a closer review of the information that has come to light in connection with the written inspection and a justification for the Data Protection Authority's decision.

3. Disclosure of the case

Køge Municipality has stated that KMD Educa Staff and KMD Educa Elev ensure rights restriction in the Aula.

Enrollment, changes and resignation of teachers are administered by the management of the individual school and take place exclusively in KMD Educa Personale. Here, it is also managed which students at which grade level the individual teacher has access to. Control of user access in Aula is done exclusively by KMD Educa Personale.

KMD Educa Personnel is managed by an employee in the School Department. Granting of rights in KMD Educa Personale takes place via Køge Municipality's user authorization form, where the immediate manager has approved the employee's access.

All authorization forms are archived in Køge Municipality's ESDH system e-Doc.

In connection with the allocation of rights to new employees, control of existing employees with rights is stored. The employee in the School Department sends the relevant head of school an email with an overview of current employees with rights and asks him to confirm that it is still accurate. A log is also kept of the creation and termination of user rights.

Køge Municipality has stated that the students are registered at the schools via www.indskrivning.dk and assigned to a class/team, whereby they are created in Uni-login. At the same time, contact persons are created and assigned to the student if they have parental authority. After this, it is the individual school's administration that is responsible for whether data about students, parents/guardians, staff and external parties are correctly registered in KMD Educa. The school's administration continuously maintains this data when the users respectively start and leave the school. When the users have been created correctly in KMD Educa, data is automatically exported every afternoon to the Danish Agency for IT and Learning's Uni-login database, SkoleGrunddata. This means that the next day the users will be associated with the school and the users will have access to the central systems with their Uni login.

Køge Municipality has also stated that the school's administration can receive advice with decisions from other authorities that can be of great importance to the registered (student). The administration ensures that the student's information is correct, and changes the set-up of the student's data if there is a need for this. All changes are registered in KMD Educa Elev. Every evening at 21.00 data is updated in the Aula. The school's administration checks the following day that the change has taken effect.

In addition, Køge Municipality has stated that Aula has another layer of user management to ensure that not everyone has access to all areas in the system.

There are two types of administrators who have rights to ensure that not everyone has access to all areas of the system: municipal administrator and institution administrator.

The municipal administrator is typically an employee of the School Department. In Køge Municipality, there are two employees who have the role of municipal administrator. One for the school area and one for the daycare area. The role gives access to all areas of Aula across all institutions.

The institution administrator role is automatically given to the head of school for the individual school. The school head can then assign the administrative staff at the school rights levels depending on the role the administrative staff at the school should have.

In conclusion, Køge Municipality has stated that the municipality has set up a working group to help the schools with the task of implementing and documenting systematic checks to a greater extent:

the school's staff (every 6 months) in KMD Educa Personale

institution administrator (every 3 months) in Aula

special arrangements for students and staff are documented and checked when notification of changes is received by the school. It can, for example, be name and address protection, parental authority, etc. Pupils and staff with special arrangements are checked in KMD Educa every 6 months.

In this connection, Køge Municipality has stated that the working group is working with a deadline of 1 January 2022, when these additional checks will be fully implemented.

4. Data Protection Authority assessment

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 for adequate security will normally entail that the data controller continuously checks whether user access to systems is limited to the personal data that is necessary and relevant for the user in question, and that the rights reflect rights restrictions in underlying systems.

According to the information provided, the Danish Data Protection Authority assumes that, in connection with the allocation of rights to new employees, checks are carried out on existing employees with rights by the School Department sending the relevant headmaster an overview of current employees with rights and asking the headmaster to confirm that it is still accurate .

The Danish Data Protection Authority finds that Køge Municipality - by not having had systematic checks, e.g. at fixed time intervals or based on random samples with the rights of users in Aula – have not taken appropriate organizational measures to ensure a level of security that matches the risks involved in the municipality's processing of personal data, cf. the data protection regulation, article 32, paragraph 1.

The Danish Data Protection Authority has emphasized that checks on the allocation of rights to new employees are not systematic, and that the municipality has not had checks on users other than employees' access to Aula, e.g. parents'.

The Danish Data Protection Authority then finds grounds to express criticism that Køge Municipality's processing of personal data has not taken place in accordance with the rules in the Data Protection Regulation, Article 32, subsection 1.

The Danish Data Protection Authority has noted that Køge Municipality has set up a working group to help the schools implement and document systematic checks of the school's staff, institution administrators and special arrangements for pupils and staff.

The Danish Data Protection Authority has also noted that the additional controls will be fully implemented on 1 January 2022.

[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).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).