Supervision of Høje-Taastrup Municipality's access rights in file systems

Date: 02-03-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Access control

Treatment safety

The Danish Data Protection Authority criticizes Høje-Taastrup Municipality for not having complied with the rules on processing security.

Journal number: 2021-423-0236

Summary

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

The inspection focused on access rights in Høje-Taastrup Municipality's file systems. In this context, a file system is the path structure the municipality stores data in on their servers. The inspection looked at whether there were differentiated rights to the various folders with information, and whether access was granted based on work-related needs.

In connection with the inspection, the Danish Data Protection Authority selected a database where access was granted for 12 AD groups, i.e. 12 groups of users.

The Data Protection Authority found that Høje-Taastrup Municipality – by not having guidelines or objective criteria for enrollment in the AD groups – had not met the rules on processing security.

The Danish Data Protection Authority emphasized that 410 people had AD access to the selected database and that the municipality could not document that an assessment had been made of the employees' work-related needs for access to the database in question.

Against this background, the Data Protection Authority criticized Høje-Taastrup Municipality.

1. Written supervision of Høje-Taastrup Municipality's processing of personal data

Høje-Taastrup 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 access rights in Høje-Taastrup Municipality's file systems, cf. Article 32 of the Data Protection Regulation.

By letter of 9 June 2021, the Data Protection Authority notified the supervisory authority of Høje-Taastrup Municipality and, in that connection, requested a list of the municipality's file systems in which information about natural persons is processed.

Høje-Taastrup Municipality issued a statement on the matter on 30 June 2021.

By letter of 11 August 2021, the Data Protection Authority requested Høje-Taastrup Municipality to provide an account of the municipality's access management to personally identifiable user data in GIS[3] in one of the municipality's drives. On this basis, Høje-Taastrup Municipality sent a supplementary opinion on the matter on 1 September 2021.

On the basis of Høje-Taastrup Municipality's statement, the Data Protection Authority requested on 13 October 2021 to receive a list of the users who were granted access via 12 AD groups to a database in GIS, with a view to carrying out a random check of the users. The Danish Data Protection Authority also requested to receive the municipality's guidelines for registration in the relevant AD groups, including an assessment of the work-related needs to have access.

Høje-Taastrup Municipality replied to the letter on 4 November 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 Høje-Taastrup 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

Høje-Taastrup Municipality has stated that the municipality uses the NTFS file system on Windows servers. Allocating access to network drives takes place via the municipality's IT department through a form. Høje-Taastrup Municipality exhibits a number of shares and limits access with NTFS rights on folders and underlying structures. NTFS permissions are assigned to AD security groups.

The IT department reports the employee's AD user into access-granting security groups upon request.

From the forwarded list of user-facing shares, it appears, among other things, that H:\ is the GIS team's dedicated network drive.

Regarding the H drive, Høje-Taastrup Municipality has stated that the data is in a shared folder 'gis' on a Microsoft Windows file server. Access to the folder is restricted via NTFS permissions. Thus, only administrators and users who are members of the AD group "gis" have access. When one of the municipality's employees logs on to a client PC with his AD user, the centrally controlled Group Policy for drive connection is interpreted, and only users who are in the AD group "gis" can connect the folder 'gis' as an H drive . In this connection, Høje-Taastrup Municipality has stated that there are 26 users on the H drive who have access, and access is only given to name and address data.

Høje-Taastrup Municipality has identified two databases that contain personal data, including LOIS, which contains social security numbers and is used for searching consultation lists etc. For the LOIS database, there is, among other things, granted access to 12 AD groups.

Høje-Taastrup Municipality has stated that there are no written down guidelines describing registration in the AD groups. Registration therefore takes place through the general user creation via an IT case management system.

In this connection, Høje-Taastrup Municipality has stated that since there are no guidelines for registration, the municipality cannot document an assessment of the work-related need. However, the municipality can document which users have used their access to the LOIS database.

Furthermore, Høje-Taastrup Municipality has stated that the LOIS database will not be exhibited to the users who have access to it. Users need to know it exists, know its name and know what software they need to use to access it.

It therefore requires relatively high technical skills to be able to use the access. Therefore, only 35 users have accessed the database in the last six months. It is also Høje-Taastrup Municipality's assessment that all 35 employees have had a work-related need for access.

Høje-Taastrup Municipality has stated that, based on the inspection, the municipality will draw up guidelines for granting access to the database.

Høje-Taastrup Municipality has forwarded a list of users who have AD access to LOIS. The list shows 410 people.

Høje-Taastrup Municipality has stated that the municipality does not have a procedure for password protection that directly

applies to file structures. The municipality has therefore forwarded a section from the security handbook on the municipality's general procedures for passwords. It appears from this:

[Exempt from publication].

4. The Danish Data Protection Authority's 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 mean that user access to systems is limited to the personal data that is necessary for the work-related needs of the user in question, and that measures have been implemented to grant and revoke access rights, so that only users who have a work-related need to have access to the information are authorized to do so.

The Danish Data Protection Authority finds that Høje-Taastrup Municipality – by not having guidelines or objective criteria for registration in the AD groups – has not taken appropriate technical or organizational measures to ensure a level of security suitable for the risks that the municipality's processing of personal data , cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has emphasized that 410 people have AD access to the LOIS database and that the municipality cannot document that an assessment has been made of the employees' work-related needs for access to the LOIS database.

The Danish Data Protection Authority then finds grounds to express criticism that Høje-Taastrup 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 notes that it cannot lead to a different result that it requires relatively high technical skills to use the access.

The Danish Data Protection Authority has noted that Høje-Taastrup Municipality intends to draw up guidelines for granting access to the database.

In this connection, the Data Protection Authority must encourage the municipality to objectively describe which function or work task must be present in order to gain access, and that a manager for this function verifies that the specific employee has this need to perform the task.

Furthermore, the Data Protection Authority finds no basis for expressing criticism of Høje-Taastrup Municipality's general procedures for passwords.

[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).

[3] Geographic Information System