Supervision of Gladsaxe Municipality's rights management in one of the municipality's systems

Date: 26-04-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Treatment safety

Access control

On the basis of an inspection focusing on the administration of access rights, the Danish Data Protection Authority has expressed criticism of Gladsaxe Municipality for not having acted in accordance with the rules on processing security.

Journal number: 2021-423-0235

Summary

Gladsaxe 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 Gladsaxe Municipality's way of managing access rights in the area of children and young people, including especially the school area. In this connection, the Data Protection Authority investigated whether Gladsaxe Municipality had revoked the access rights of resigned employees to the municipality's electronic case and document management system SBSYS.

The Danish Data Protection Authority found that Gladsaxe Municipality had not acted in accordance with the rules on processing security.

The Data Protection Authority emphasized that Gladsaxe Municipality had not taken away a user's access rights to SBSYS after the employee's resignation, and that the municipality had not undertaken follow-up or control of terminated employees' rights.

Against this background, the Data Protection Authority criticized Gladsaxe Municipality.

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

Gladsaxe 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 Gladsaxe Municipality's way of administering access rights in the area of children and young people, including especially the school area, cf. the data protection regulation, article 32, subsection 1.

By letter of 9 June 2021, the Data Protection Authority notified the supervisory authority of Gladsaxe 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.

Gladsaxe Municipality issued a statement on the matter on 1 July 2021.

On the basis of the opinion, the Data Protection Authority chose to carry out further checks of Gladsaxe Municipality's rights management in the municipality's ESDH system SBSYS.

On 11 August 2021, the Danish Data Protection Authority requested Gladsaxe Municipality to disclose which personal data the municipality processes in SBSYS in the school area, how the municipality creates and terminates users in SBSYS, and how the municipality removes rights in the system when employees' functions change. On that basis, Gladsaxe Municipality sent a supplementary opinion on the matter on 1 September 2021.

After a review of Gladsaxe Municipality's supplementary response of 1 September 2021, the Danish Data Protection Authority requested on 13 October 2021 to receive a list of resigned employees at the individual schools in the 2nd quarter of 2021, with a view to the Danish Data Protection Authority's selection of users for random checks.

On 3 November 2021, Gladsaxe Municipality sent a list of resigned employees in the 2nd quarter of 2021 in the school area.

Against this background, the Danish Data Protection Authority requested on 17 November 2021 Gladsaxe Municipality for documentation of when 13 selected employees' access rights to SBSYS were revoked.

By letter of 7 December 2021, Gladsaxe Municipality stated that 12 out of the 13 users had not been created in SBSYS, and that the one created employee did not have access for a long time before termination.

The Danish Data Protection Authority then requested, by letter of 9 March 2022, to receive a list of resigned employees in the organizational units (at the individual schools) in the 4th quarter of 2021, which had been created in SBSYS, before resignation for the purpose of the Danish Data Protection Authority's selection of users for random checks.

Gladsaxe Municipality replied to the letter on 6 April 2022.

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 Gladsaxe Municipality's processing of personal data has not taken place in accordance with the rules in Article 32, subsection 1 of the Data Protection Regulation.

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

3.1.

It appears from the section on access management in Gladsaxe Municipality's information security handbook that it must be ensured that access to the municipality's IT systems, servers, networks, shared mailboxes, shared drives and PCs is restricted through concrete authorizations. The level of authorization is determined on the basis of a specific assessment of business-related requirements and the sensitivity of the information, and specific legislative obligations in relation to data access must be observed in particular. It must be ensured that employees only have access to personal data or confidential data for which the employee has a functional need.

It also appears from the information security handbook that all authorization on the municipality's IT systems, networks, servers and other IT equipment must be done with a unique and personal user ID. The user ID must be traceable to the person responsible for a given activity. When establishing joint accounts in special cases, a concretely documented risk assessment is required.

The following is stated about the allocation of user access in the information security manual:

"The responsibility for granting authorizations is between The digitization department and the system owners. The procedure is determined by the individual system owner, and the assignment of rights must always be documented.

The digitization department prepares a general procedure for creating, assigning, changing and deleting access. For the individual systems, mailboxes, drives and other data, the owner is responsible for drawing up and complying with the procedure based on the general procedure, all control of access must be documented.

System owner, mailbox owner, drive owner and data owner can decide that authorizations can be done via role profiles, and it is the system owner's responsibility to create and maintain the role profiles. The system owner is responsible for ensuring that

role profiles do not provide access to data for which the profile was not intended.

Procedures for authorizing user access must include a formal authorization form specifying the required privileges. The form can be in both digital and analogue form, just as forms can be signed electronically, e.g. by sending the form via email.

When creating or resetting passwords, the employee must be assigned a temporary password, which the employee must change upon first use."

Regarding the review of users' access rights, the following appears:

"A review of users and their rights must be carried out in all systems, mailboxes and drives. The method and frequency must be determined in a specific risk assessment. However, the frequency must not exceed every 18 months.

Reviews of user accounts are initiated by the system owner, and follow-ups must be documented in writing.

However, review of whether resigned employees have an active user account must always be reviewed completely."

In addition, the following appears on the withdrawal or adjustment of access rights:

"When an employee changes tasks or gets a different organizational affiliation, an assessment of the employee's authorizations and access must be carried out so that these continue to reflect the employee's needs. It is the original boss who is responsible for the termination of rights and the subsequent boss who is responsible for the allocation.

When the employee resigns, all IT equipment must be included. User profiles and authorizations are deactivated or deleted according to the municipality's procedure for assigning, changing and deleting authorizations. It is the immediate manager's responsibility to report to the authorizing functions.

When users are terminated, automated runs (batch runs) can be used, which, based on records about the employee's employment, carry out automated deletions of users. User accounts can be deactivated after a specified period of user inactivity, so that the user can only log in after requesting reactivation. Accounts that are deactivated can be deleted after a specified period of time. In the cases mentioned, written approval of the user termination is not required.

In the event of expulsion, dismissal or dismissal of an employee, the employee's access rights must be revoked immediately after a specific assessment and on the recommendation of the immediate manager.

In the event of leave or other prolonged absence, the user's access rights must be deactivated, unless the employee's manager allows specific access to remain active."

It also appears from the information security handbook that all potential access to personal data must be logged. This means

that all failed and successful logins must be able to be associated with a unique user. Access to log information about the behavior of Gladsaxe Municipality's users must be available to the municipality's administrators.

3.2.

It appears from the case that SBSYS is an ESDH system that Gladsaxe Municipality uses in the school area for journaling e.g. action plans, student plans, reports, educational readiness assessments and case files, etc. Gladsaxe Municipality has stated that the municipality i.a. processes contact information, social security numbers, health information, test information and information about school affiliation, social conditions, ethnicity and criminal conditions in SBSYS in the school area.

Gladsaxe Municipality has stated that in the school area in the municipality it is managers and the administrative staff at the schools, as well as the school department staff at the town hall, who have access to SBSYS.

It is the individual manager in the organizational units (at the individual schools) who may via a super user orders/approves that an employee must have access to SBSYS. In practice, this happens when the manager has decided which parts of his or her organization should use SBSYS and what role the employees should have in SBSYS. These organizational units (places of employment) are thus authorized to access SBSYS. In some cases, this access only applies to individual employees in an organizational unit, and here only the relevant employees who are authorized to access SBSYS – or to a specific role in SBSYS.

Gladsaxe Municipality has stated that the authorization for SBSYS takes place via Gladsaxe Municipality's AD (Active Directory). Organizational units and employees are continuously synchronized from the municipality's virtual organizational chart GLASNOST to AD and further into/out of SBSYS. This means that users who are terminated in AD no longer have access to SBSYS. This also means that users who do not have access to a computer on the municipality's domain also do not have access to SBSYS.

When a user's access is terminated in SBSYS, the user is not deleted, but the user is deactivated to ensure transparency in e.g. previous log information.

Gladsaxe Municipality has also stated that the administration/access management itself, i.e. assignment and removal of membership in security groups and roles in SBSYS is done via AD and is carried out by a Hotline function in Gladsaxe Municipality's IT department. This is done on the basis of order forms which are filled in by super users in the administrations on behalf of the local manager. Via the forms, only the super users have the opportunity to order and cancel rights, e.g. when

users change organizational roles. It is the individual manager who is responsible for ensuring that their employees have the correct roles in SBSYS, and therefore also the individual manager's responsibility to ensure that the rights are only assigned according to a work-related need.

When a user moves organizational location, it is the responsibility of superusers in the transferring organizational unit to unregister the user's affiliation/role from old security groups. Superusers associated with the receiving organizational unit are responsible for ordering/enrolling the user's association/role into new relevant security groups.

It appears from the case that there were two terminated employees in the school area in Gladsaxe Municipality, who were established in SBSYS before resignation in the 4th quarter of 2021.

It also appears from the case that Gladsaxe Municipality has, on its own initiative, investigated dates for deactivation in the municipality's payroll system and administrative AD, which i.a. has given access to SBSYS.

Gladsaxe Municipality established in this connection that the user [X] was deactivated in the payroll system with retroactive effect. This contributed to the fact that the user was not shut down in time in relation to the latest date of employment.

Gladsaxe Municipality has also investigated whether the user has been active in SBSYS, which was not the case.

4. The Danish Data Protection Authority's assessment

The Danish Data Protection Authority assumes that the user [X] has had access to SBSYS after the employee's resignation.

The Danish Data Protection Authority also assumes that the procedure in the information security handbook, that review of whether resigned employees have an active user account must always be reviewed in full, was not followed in the case in question.

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 measures have been implemented to grant and revoke access rights to systems, 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 Gladsaxe Municipality – by not having taken away user [X]'s access rights to SBSYS after the employee's resignation, and by not having carried out the necessary follow-up or revision of terminated employees' rights – has not taken appropriate technical and organizational measures for to ensure a level of security that suits the risks involved in the municipality's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority is of the opinion that, in addition to a procedure for withdrawal of rights upon termination of employment, there must be a control procedure that effectively follows up on whether this has also taken place.

This control procedure must be organizationally and/or technically anchored, so that it is not carried out due to human error

The Danish Data Protection Authority then finds grounds to express criticism that Gladsaxe Municipality'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).

[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).