Supervision of Gentofte Municipality's rights management in departmental and functional mailboxes

Date: 28-01-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Access control

Treatment safety

The Danish Data Protection Authority has expressed criticism that Gentofte Municipality has not carried out sufficient checks on the rights in the municipality's departmental and functional mailboxes.

Journal number: 2021-423-0238

Summary

Gentofte Municipality was among the authorities that the Data Protection Authority had selected in the summer of 2021 to supervise under the Data Protection Regulation and the Data Protection Act.

The Danish Data Protection Authority's inspection was a written inspection which focused on Gentofte Municipality's rights management for e-mail mailboxes to which several users have access, typically called departmental and functional mailboxes.

The Danish Data Protection Authority found that Gentofte Municipality had not carried out the necessary checks on whether the access rights to the municipality's departmental and functional mailboxes were correct, which was not in accordance with the rules on processing security.

The Danish Data Protection Authority emphasized that Gentofte Municipality only checked two mailboxes out of 564 in the latest quarterly sample.

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

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

Gentofte Municipality was among the authorities that the Data Protection Authority had selected in the summer of 2021 to supervise according to the data protection regulation0F0F[1] and the data protection law1F1F[2].

The Danish Data Protection Authority's inspection was a written inspection which focused on Gentofte Municipality's rights

management in departmental and functional mailboxes, cf. the data protection regulation, article 32, subsection 1.

By letter of 10 June 2021, the Data Protection Authority notified the supervisory authority of Gentofte Municipality. In this connection, the Danish Data Protection Authority requested to be sent a list of the municipality's departmental and functional mailboxes, in which information about natural persons is processed.

Gentofte Municipality issued a statement on the matter on 30 August.

On the basis of the statement, the Data Protection Authority decided to carry out further checks with the mailboxes "smittepospring@gentofte.dk" and "Elverhoj2@gentofte.dk".

By letter of 13 October 2021, the Data Protection Authority requested Gentofte Municipality to forward a list of who has access to the mailboxes. The Danish Data Protection Authority also requested Gentofte Municipality to provide information on which personal data the municipality processes in the mailboxes in question, and how the arrival and departure of users is regulated, and which control measures the municipality has in place to see if resigned users have had access to the mailboxes removed.

Gentofte Municipality replied to the letter on 29 October 2021.

On 17 November 2021, the Danish Data Protection Authority asked Gentofte Municipality to send documentation for the most recent check carried out for the mailboxes "smittepospring@gentofte.dk" and "Elverhoj2@gentofte.dk".

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 Gentofte 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

At the outset, Gentofte Municipality has stated that the processing activities generally take place in the relevant professional system and not in departmental or functional mailboxes. However, ordinary, sensitive or confidential personal data, including social security numbers, can and will be processed in many of the mailboxes, depending on the work tasks of the individual department/function. Sensitive and confidential information in departmental and functional mailboxes will preferably be available in the form of inquiries from citizens, companies and other authorities who wish to get in touch with the municipality.

Gentofte Municipality has sent lists of the municipality's departmental and functional mailboxes divided by the respective tasks the mailboxes are used for. The list is divided into public mailboxes and shared mailboxes, and Gentofte Municipality has stated that the rights management is the same, but the underlying technology is different. Access to both types of mailboxes is granted by adding the IT users' unique AD account to the individual mailbox. It appears from the list that there are 387 public mailboxes and 177 shared mailboxes.

It appears from Gentofte Municipality's procedure for granting rights to mailboxes (user administration) that the starting point is that employees are only assigned a personal mailbox upon employment in the municipality. Access to other relevant mailboxes is granted after contacting the IT service desk. The inquiry must take place digitally via ServiceNow. For inquiries by telephone, please refer to ServiceNow, as no rights may be assigned on the basis of inquiries made by telephone.

It also appears that the manager or an authorized manager requests the allocation of rights via a ticket in the ServieNow help desk system. The manager/authorized manager must specify which mailboxes the employee must have rights to. An employee from the user administration team then assigns rights to the desired mailboxes. The case can also be sent to the user administration team via a rights form, in which the manager/authorized manager states which mailboxes the IT user must have rights to. Furthermore, it is not possible to assign rights to oneself, regardless of whether one is a manager or authorized manager.

Gentofte Municipality has stated that the mailbox smitteopsporing@gentofte.dk was created as part of the conclusion of an agreement with the Swedish Agency for Patient Safety regarding municipal assistance for infection detection to prevent the spread of infection by covid-19. The mailbox has been used to receive data (infection tracking lists) for use in the performance of tasks, including name, address, social security number, infection ID, telephone number and date of most positive. The lists have been redistributed through a secure channel and then deleted.

Gentofte Municipality has stated that eight employees who are part of the task of covid-19 infection detection have access to the mailbox.

About the mailbox elverhoj2@gentofte.dk, Gentofte Municipality has stated that the mailbox belongs to Børnehuset Elverhøj, which is a combined kindergarten and nursery. The mailbox is used, among other things for the institution to receive a message from the place instruction that a child has been given a place in the institution, where the names of the parents and the child appear. The mailbox is also used for parents to make inquiries because they want a tour of the institution. They

typically state their name and telephone number. In addition, the mailbox is also used for unsolicited applications, which are forwarded to the manager's own email and deleted.

Gentofte Municipality has stated that two employees, who are both managers, have access to the mailbox.

In addition, Gentofte Municipality has stated that rights to mailboxes are ordered via a rights form, which is filled in by the manager or the manager's representative. Departure is done by using the deletion form. Both parts are handled by the user administration team in the IT department and the processes are described in forwarded procedures.

Gentofte Municipality has also stated that when employees leave, access to mail and mailboxes is immediately deactivated.

According to new guidelines, the user administration team carries out quarterly random checks of mailboxes, whereby the manager responsible for a mailbox is sent an overview of employees in that mailbox for the purpose of verification.

In addition, Gentofte Municipality has stated that the samples are carried out based on the municipality's total number of mailboxes in accordance with new guidelines. The status of the samples was that in the fourth quarter of 2021, Gentofte Municipality had carried out checks on two mailboxes, which were selected based on the expectation of sensitivity in data based on naming. The mailboxes smitteopsporing@gentofte.dk and Elverhoj2@gentofte.dk were not sampled. Gentofte Municipality has stated that the accesses to the mailboxes smitteopsporing@gentofte.dk and Elverhoj2@gentofte are correct, as the employees in question all have a service purpose in accessing the two mailboxes.

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 the data controller continuously checks whether access rights to departmental and functional mailboxes are limited to the personal data that is necessary and relevant to the work-related needs of the user in question.

In addition, the Danish Data Protection Authority is of the opinion that the control of access rights should, normally as a minimum, consist of a verification of the work-related need at the time of allocation, an ongoing control based on verification

that this need is still present and some form of auditing thereof. If the auditing is carried out as random checks, the number of random samples taken must be representative in relation to the number of possible incidents and the risk to the rights of the data subjects.

The Danish Data Protection Authority finds that Gentofte Municipality's control scope in relation to the number of rights groups, specifically by not carrying out sufficient checks on the access rights to the municipality's departmental and functional mailboxes - has not taken appropriate organizational measures to ensure a level of security that fits the risks that are in the municipality's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Norwegian Data Protection Authority has emphasized that Gentofte Municipality only checked two mailboxes out of 564 in the most recent quarterly sample.

The Norwegian Data Protection Authority notes that it is the immediate assessment of the authority that Gentofte Municipality has not demonstrated that, based on the risks involved in the municipality's processing of personal data, two random samples per quarter are sufficient given the number of mailboxes in total.

The Danish Data Protection Authority then finds grounds to express criticism that Gentofte 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 encourages Gentofte Municipality to intensify its control of rights management in the municipality's departmental and functional mailboxes.

The Danish Data Protection Authority has also found that Gentofte Municipality's procedures in connection with the allocation and withdrawal of rights to the municipality's mailboxes are generally appropriate.

[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).