Adequate access control procedures but non-compliance

Date: 30-11-2021

Decision

Public authorities

Criticism

Supervision / self-management case

Access control

Treatment safety

Logging

The Danish Data Protection Authority has expressed criticism that Allerød Municipality has not followed its own guidelines for control. However, the municipality's procedures for random checks were generally satisfactory.

Journal number: 2021-423-0234.

Summary

Allerød 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 Allerød Municipality's way of administering access rights in the social administration. In connection with the inspection, the Danish Data Protection Authority asked Allerød Municipality for documentation of samples carried out in one of the municipality's systems.

The Data Protection Authority found that Allerød Municipality's procedures for random checks of the log in the social administration's systems were generally satisfactory in relation to the risk picture.

It was in this connection the Danish Data Protection Authority's assessment that sample checks every six months constitute the absolute minimum of checks in systems that process a lot of confidential and sensitive personal data, or where the access rights are of a broader nature.

However, the Norwegian Data Protection Authority found that the municipality had not followed its own guidelines for control in at least one case.

Against this background, the Danish Data Protection Authority expressed criticism that Allerød Municipality's processing of

personal data had not taken place in accordance with the rules on processing security.

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

Allerød Municipality was among the public 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 Allerød Municipality's way of administering access rights in the social administration, cf. Article 32 of the Data Protection Regulation.

By letter of 9 June 2021, the Data Protection Authority notified the supervisory authority of Allerød Municipality. In this connection, the Data Protection Authority requested to be sent a list of systems in the municipality's social administration, in which information about natural persons is processed, and about the municipality's policies for audits and samples for unauthorized access attempts.

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

On 11 August 2021, the Data Protection Authority Allerød Municipality requested documentation for samples carried out in one of the municipality's systems. Against this background, the municipality sent a supplementary statement in the case on 31 August 2021.

2. The Data Protection Authority's decision

After the inspection of Allerød Municipality, the Data Protection Authority finds reason to conclude in summary:

That Allerød Municipality's procedures for random checks of the log in the social administration's systems are generally satisfactory in relation to the risk picture.

That Allerød Municipality has not followed the municipality's own guidelines for control in at least one case.

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

Allerød Municipality has stated that the social administration in the municipality is organizationally located in the Civic Service and Families departments.

It appears from the submitted lists that the social administration uses a number of different systems where ordinary personal data, sensitive data and other data worthy of protection are processed, including social security numbers.

Allerød Municipality has stated that employees of the municipality may only be authorized to have access to IT systems that they need in connection with their ordinary work. When an employee must have access to an IT system, access must be restricted so that the person concerned only has access to see and work with the matters that are necessary to be able to carry out the specific core task.

The heads of the areas are responsible for approving user registration and de-registration at the municipality's IT service desk.

It appears from Allerød Municipality's guidelines for logging and sampling that checks of systems subject to logging in Citizen Service are carried out using random samples that are taken on average every 6 weeks. The samples fall at different intervals, e.g. 1 month, 2½ months, 5 months, 3 months, etc., but no more than 6 months. The dates appear in an appendix to which only security staff have access.

A sample includes 5-6 posts made 1-3 days before the employee is asked to explain the reason for the posts.

The samples are printed and submitted to the employees who made the postings. The employees note the reason for the postings. The samples and notes are then submitted to the manager who has the greatest insight into the person's work. If this gives rise to questions, the boss talks to the employee, otherwise the check is considered to have been carried out with satisfactory results.

On the basis of Allerød Municipality's statement of 30 June 2021, the Danish Data Protection Authority chose to carry out further checks of the municipality's sampling in the ESDH system Acadre. The Danish Data Protection Authority therefore asked Allerød Municipality by letter of 11 August 2021 to send documentation for samples carried out in Acadre for the past year.

Allerød Municipality has stated that all withdrawals are made centrally by the administrator for Acadre, who is organizationally located in the Secretariat. The responsibility for carrying out the inspection rests with the manager and should be carried out twice a year.

In this connection, the municipality has stated that all extracts must be reviewed in order to check whether the municipality's employees still have the access necessary for them to carry out their work - and no more than that.

Allerød Municipality has also stated that, due to the Covid-19 situation, no samples have been taken in the period from 25

September 2020 until 13 August 2021, and normal operations will be re-established from September 2021.

It appears from the sent sample check in Acadre for Citizen Service and Families that Allerød Municipality on 24 June 2020, 25 September 2020 and 13 August 2021 has checked the log of 3-9 employees' viewing of e.g. cases and documents in Acadre.

4. The Danish Data Protection Authority's assessment

The Danish Data Protection Authority assumes that Allerød Municipality generally logs the use of personal data in the municipality's IT systems, including in the Acadre system.

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 regularly conducts random samples of the log to check that users only access information that they have a work-related need for, and that measures have been implemented regarding the allocation and deprivation of 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 no basis for overriding Allerød Municipality's assessment that random checks take place twice a year.

However, the Danish Data Protection Authority is of the opinion that sampling every six months constitutes the absolute minimum of control, in systems that process a lot of confidential and/or sensitive information, or where the access rights are of a broader nature.

According to the information provided, the Danish Data Protection Authority assumes that Acadre is a system with these types of information.

In addition, in accordance with Allerød Municipality's own explanation, the inspection assumes that no random checks have been carried out in the Acadre system in the period 25 September 2020 to 13 August 2021.

The Danish Data Protection Authority finds that Allerød Municipality – by not having checked the log in Acadre for more than six months – has not taken appropriate organizational measures to ensure a level of security that matches the risks that the

municipality's processing of personal data, cf. Article 32, subsection of the data protection regulation. 1.

The Danish Data Protection Authority has hereby emphasized that Allerød Municipality has carried out inspections on 24 June 2020, 25 September 2020 and 13 August 2021.

The fact that the employees have been sent home and worked from home during the Covid-19 situation cannot lead to a different assessment that checks should take place at least every six months.

The Norwegian Data Protection Authority also finds it striking that Allerød Municipality has carried out the latest check two days after the authority's letter of 11 August 2021, in which the authority requested documentation for samples carried out in Acadre for the past year.

The Norwegian Data Protection Authority has noted that normal operations have been re-established from September 2021.

5. Conclusion

After the inspection of Allerød Municipality, the Data Protection Authority finds reason to conclude in summary:

That Allerød Municipality's procedures for random checks of the log in the Social Administration's systems are generally satisfactory in relation to the risk picture.

That Allerød Municipality has not followed the municipality's own guidelines for control in at least one case.

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

[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).