Serious criticism of Mariagerfjord Municipality

Date: 15-07-2022

Decision

Public authorities

Serious criticism

Injunction

Supervision / self-management case

Access control

Treatment safety

Basic principles

Logging

Password

Risk assessment and impact analysis

On the basis of an inspection with a special focus on maturity in the security area, the Data Protection Authority expresses serious criticism of Mariagerfjord Municipality.

Journal number: 2022-423-0261

Summary

The Danish Data Protection Authority carried out an inspection of Mariagerfjord Municipality in June. The purpose of the inspection was, among other things, to make an overall assessment of the municipality's maturity in relation to data protection, particularly in the area of security.

On the basis of the inspection, the Data Protection Authority found grounds to state:

serious criticism that Mariagerfjord Municipality had stored personal data beyond what was necessary in relation to the purpose, and by not having introduced guidelines or equivalent organizational measures for deleting the personal data in cases where technical measures were not possible.

serious criticism that Mariagerfjord Municipality had not taken appropriate security measures to ensure a level of security suitable for the risks involved in the municipality's processing of personal data.

The Danish Data Protection Authority issues orders

On the basis of the inspection, the Data Protection Authority has found grounds to notify Mariagerfjord Municipality of an order to prepare a list of the municipality's systems in which personal data is processed, to delete personal data where it is no longer necessary for the municipality to store the information and to prepare a plan for how the municipality, in cooperation with the municipality's system suppliers, can have personal data deleted in the municipality's systems, which the municipality no longer has a purpose to store.

The Danish Data Protection Authority has also found occasion to notify Mariagerfjord Municipality of an order to remove employees' rights to install programs and execute harmful code, etc. on the computers and devices that can be connected to the municipality's network.

Decision

The Danish Data Protection Authority hereby returns to the matter, where the Danish Data Protection Authority announced on 11 May 2022 a physical inspection visit to Mariagerfjord Municipality.

The inspection focused on Mariagerfjord Municipality's compliance with articles 5 and 32 of the data protection regulation[1], based on the municipality's response of 10 September 2021 in the inspection's maturity analysis and the municipality's statement of 19 January 2022.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that Mariagerfjord Municipality's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 5, subsection 1, letter e and Article 32, subsection 1.

The Danish Data Protection Authority also finds grounds to notify Mariagerfjord Municipality of an order to:

to prepare a list of the municipality's systems in which personal data is processed. The list must contain information on whether the individual system can delete, and if so how, and what deletion deadlines are for the system in question.

to delete personal data that has exceeded the deletion deadlines set by Mariagerfjord Municipality and where it is no longer necessary for the municipality to store the information, to the extent that the personal data can be deleted manually or automatically,

to prepare a plan for how Mariagerfjord Municipality, in cooperation with the municipality's system suppliers, can have personal

data deleted from the municipality's systems, which the municipality no longer has a purpose to store.

The deadline for compliance with the order is 15 November 2022. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter d.

At the same time, the Data Protection Authority also finds grounds to notify Mariagerfjord Municipality of an order to remove employees' rights to install programs and execute harmful code, etc. on the computers and devices that can be connected to the municipality's network.

The deadline for compliance with the order is 15 August 2022. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act[2] § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter d.

The orders are announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

As part of the Danish Data Protection Authority's ongoing supervisory activities, which include carried out through random checks, Mariagerfjord Municipality was notified on 9 July 2021 that the municipality had been selected for a planned inspection.

The inspection was initially carried out as a questionnaire survey. The purpose of the inspection was, among other things, that the Data Protection Authority could make an overall assessment of the municipality's maturity in relation to data protection, particularly in the area of security. In continuation of the answers given, the Danish Data Protection Authority would possibly request documentation, ask further questions, initiate further random checks or notify a physical inspection visit.

Mariagerfjord Municipality answered the questionnaire on 10 September 2021. After a review of the municipality's response, the Danish Data Protection Authority found that the municipality stated for a number of questions that the activities were not, or were only partially, completed.

Against this background, the Danish Data Protection Authority requested the municipality on 8 December 2021 to send an annual overview of all activities which, at the time of answering the questionnaire, were planned or partially implemented.

Mariagerfjord Municipality replied to the letter on 27 January 2022.

By letter of 4 February 2022, the Data Protection Authority requested a supplementary statement in the case, which Mariagerfjord Municipality responded to on 15 March 2022.

On the basis of Mariagerfjord Municipality's response to the questionnaire and the municipality's statements of 27 January 2022 and 15 March 2022, the Data Protection Authority announced an inspection visit to Mariagerfjord Municipality on 11 May 2022.

The inspection visit to Mariagerfjord Municipality was carried out on 7 June 2022.

2.1. Mariagerfjord Municipality's comments

Mariagerfjord Municipality has stated that the municipality has not made actual charts of threats and consequences, but that the municipality has been out in the individual administrations and included the experiences and observations from there in the risk work.

It appears from Mariagerfjord Municipality's response to the questionnaire that the municipality has only partially implemented two-factor authentication for access to systems and databases where personal data is stored and processed.

Mariagerfjord Municipality has stated during the inspection visit that multi-factor authentication will be implemented from the new year.

Mariagerfjord Municipality has stated about the control of access rights that control is done by a manual process. The municipality has approx. 300 systems with personal data, and the data protection advisor sends a six-monthly list of systems in which authorization checks must be carried out to the system owners, after which they have approx. 6 weeks to check that the employees who have been granted access to the systems have the correct rights.

In this connection, Mariagerfjord Municipality also stated that as soon as an employee is no longer employed (retired in the payroll system), their access to both the network and the subject systems managed via the municipality's IdM is taken away. If employees change departments in the payroll system, the rights are also withdrawn when the changes in employment take place in the payroll system.

Mariagerfjord Municipality has stated that the municipality has not generally introduced systematic log follow-up, but that the

municipality carries out random checks of the administrators' logs. The municipality has primarily used logs if there has been a reason, e.g. in case of suspected abuse or during audit checks.

Mariagerfjord Municipality has also stated that, on the basis of a risk assessment, a management decision has been made that employees have rights to install programs on their own devices, and that employees are greeted with a pop-up message that warns the employee before the program be picked up.

In addition, Mariagerfjord Municipality has stated that many of the municipality's systems are not geared for automatic deletion, and only a few systems support anything other than deletion at single entry level in the database. It is often about information that goes back a long way, and the municipality has no alternatives to the systems. The municipality has been in contact with the suppliers of the systems to no avail. Mariagerfjord Municipality also stated that there are system terms that only support manual deletion, but where no deletion takes place.

3. Reason for the Data Protection Authority's decision

3.1.

The Danish Data Protection Authority assumes - in accordance with what Mariagerfjord Municipality explained - that the municipality processes personal data that should have been deleted, but where deletion has not taken place, either because the system terms do not support deletion, or because they only support manual deletion, and where a such manual deletion has not occurred. The Danish Data Protection Authority also assumes that Mariagerfjord Municipality does not have a comprehensive overview of the systems in which such processing takes place.

This appears from the data protection regulation's article 5, subsection 1, letter e, that personal data must be stored in such a way that it is not possible to identify the data subjects for a longer period of time than is necessary for the purposes for which the personal data in question is processed.

The Danish Data Protection Authority finds that Mariagerfjord Municipality - by having stored personal data beyond what was necessary in relation to the purpose, and by not having introduced guidelines or equivalent organizational measures for deleting the personal data where technical measures were not possible - has not acted in accordance with the data protection regulation, article 5, subsection 1, letter e.

The Norwegian Data Protection Authority notes that a lack of system technical support cannot lead to the principle of storage limitation in the Data Protection Regulation, Article 5, subsection 1, letter e, is set aside.

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that Mariagerfjord Municipality's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 5, subsection 1, letter e.

The Danish Data Protection Authority also finds grounds to notify Mariagerfjord Municipality of an order to:

to prepare a list of the municipality's systems in which personal data is processed. The list must contain information on whether the individual system can delete, and if so how, and what deletion deadlines are for the system in question.

to delete personal data that has exceeded the deletion deadlines set by Mariagerfjord Municipality and where it is no longer necessary for the municipality to store the information, to the extent that the personal data can be deleted manually or automatically,

to prepare a plan for how Mariagerfjord Municipality, in cooperation with the municipality's system suppliers, can have personal data deleted from the municipality's systems, which the municipality no longer has a purpose to store.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

The deadline for compliance with the order is 15 November 2022. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letters d and e.

3.2. 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 regularly carries out random samples of the log to check that users only access information that they have a work-related need for.

In addition, 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 user access to systems is limited to the personal data that is necessary and relevant for 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 and frequency 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.

Furthermore, the Danish Data Protection Authority is of the opinion that the requirement for adequate security will normally mean that the data controller, when creating remote access to IT systems where data is processed

sensitive and confidential personal data, must have implemented measures for verification, such as certificate, multi-factor login or other similar measure for verification. This is particularly relevant where access is created from a network that is not subject to the data controller's control.

In addition, the Danish Data Protection Authority is of the opinion that the requirement for adequate security will normally mean that employees do not have rights to install programs on their own mobile devices and computers that have access to the network where production data is accessed, as the possibility of local execution can provide an unnecessary attack point for unauthorized access, ransomware attacks and installation of backdoors or other malicious code.

Based on the above, the Danish Data Protection Authority finds that Mariagerfjord Municipality - by not checking log summaries, by not having implemented multi-factor authentication or another additional layer of verification, and by not having limited employees' rights to install programs on their devices - has not taken appropriate organizational and technical measures to ensure a security level that matches the risks involved in the municipality's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

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

At the same time, the Data Protection Authority also finds grounds to notify Mariagerfjord Municipality of an order to remove employees' rights to install programs and execute harmful code, etc. on the computers and devices that can be connected to

the municipality's network.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

The deadline for compliance with the order is 15 August 2022. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letter d.

The Data Protection Authority must also recommend that Mariagerfjord Municipality checks access rights to the municipality's systems with personal data with a more frequent frequency than every six months, and that Mariagerfjord Municipality conducts random checks of log information.

[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).