Serious criticism of Coop Danmark A/S' processing of information on the company's shared drive

Date: 04-11-2021

Decision

Private companies

Serious criticism

Reported breach of personal data security

Unauthorized access

Access control

Treatment safety

The Danish Data Protection Authority has expressed serious criticism that Coop Danmark A/S has not met the requirement for necessary security measures in Article 32 of the Data Protection Regulation.

Journal Number: 2021-441-9356.

The Danish Data Protection Authority hereby returns to the case where Coop Danmark A/S reported a breach of personal data security to the Danish Data Protection Authority on 12 June 2021. The report has the following reference number: bf3548a01674bfdb09e5472d3c1cbf776494b2fd.

Coop Danmark A/S then submitted a follow-up notification on 3 September 2021 and, at the Data Protection Authority's request, appeared on 8 October 2021 with a statement in the matter.

Summary

The Danish Data Protection Authority has made a decision in a case where Coop has reported a breach of personal data security to the Danish Data Protection Authority.

Coop had become aware that personal data had been placed on the company's shared drive without sufficient access control. The information concerned a total of 477 employees and external consultants. Coop discovered the breach in connection with the company testing a new scanning tool.

The Danish Data Protection Authority found that Coop has not met the requirement for necessary security measures, because the company should have been aware earlier that employees could have mistakenly placed personal data on the company's shared drive. The company should therefore, in the Data Protection Authority's opinion, have checked and cleaned up the

company's shared drive and introduced relevant security measures at an earlier stage.

The Norwegian Data Protection Authority also found that Coop reported the security breach to the authority in a timely manner, as the notification was made within the time limit of 72 hours.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that Coop Danmark A/S' processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

The Danish Data Protection Authority also finds that Coop Danmark A/S has acted in accordance with the data protection regulation's article 33, subsection 1.

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

2. Case presentation

It appears from the material submitted by Coop Danmark A/S that the company became aware on 9 June 2019 that files with personal data had been placed in folders on the company's shared drive without sufficient access control. Some of the information had been placed in the folders by the registered persons themselves, while other information had been placed by Coop Danmark A/S as part of the employment. The oldest documents were placed on the shared drive in 2013.

The information concerned a total of 477 employees and external consultants. For 20 of these persons the information concerned the persons' health, for 10 persons the information referred to the persons' professional affiliation, for 46 persons the information referred to the persons' financial circumstances in connection with remuneration, compensation, subsidies and payment for services, and for 474 persons the information referred to the persons' social security numbers.

Coop Danmark A/S discovered the breach in connection with the company testing a new scanning tool. The tool was set to search for social security numbers and credit card numbers. The scan identified 35 files, which were placed in quarantine on 11 June 2021. This meant that the files were moved to a folder where only employees who work on a daily basis with handling security breaches in Coop Danmark A/S could access them. However, running the scan tool was found to have failed correctly as the number of files found was not complete. Consequently, work was subsequently carried out with a reconfiguration. After the technical challenges were resolved, the scan tool was run again on August 24, 2021 with the same criteria. In this connection, an additional 266 files that met the criteria for the scan were identified. These new files were placed in quarantine

on 28 August 2021. It has been necessary for Coop Danmark A/S after both the first and second scan to manually review each individual file identified by the scanning tool, as the company is aware that the scanning tool false positive results may occur and the same information may appear several times.

Coop Danmark A/S has submitted a copy of the company's policy from December 2019 regarding access control and user management and the company's process for managing user rights. It appears from this that in the company it is not possible for the individual employee to create a folder on a shared drive. This can only be done through a request to a service function in Coop Danmark A/S' IT department. Access is granted based on the principle of work-related need.

In Coop Danmark A/S' view, this process has largely worked. The company justifies this by saying that the personal data in question was found on a file drive containing over 17 terabytes of data. Coop Danmark A/S has also referred to the fact that the personal data relates to 2013-2017, when there was not the same policy for user management as today.

Notification of all affected data subjects was initiated on 3 September 2021.

In conclusion, Coop Danmark A/s has assessed that the previous approach to handling shared files can be improved, which is why the company has been preparing for the transition to a different and better way of handling such data for some time. Coop Danmark A/S is in a process which aims to close down joint drives in the traditional sense in order to transition to a more secure solution, where, among other things, will be a better user management and logging. It is therefore also the company's expectation that the risk of similar breaches will be reduced in the future.

3. Reason for the Data Protection Authority's decision

Based on what Coop Danmark A/S provided, the Danish Data Protection Authority assumes that information on 477 natural persons has been available on the company's shared drive, and that the oldest information has been available since 2013. The Danish Data Protection Authority also assumes that Coop Danmark A /S has cleaned up the files from 11 June 2021 until 28 August 2021, and that these were moved to a folder where only employees with a work-related need had access to the information.

On this basis, the Danish Data Protection Authority assumes that there has been unauthorized access to personal data, which is why the Danish Data Protection Authority finds that there has been a breach of personal data security, cf. Article 4, No. 12 of the Data Protection Regulation.

3.1. Article 32 of the Data Protection Regulation

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 cf. Article 32 for adequate security will normally mean that in systems with a large amount of information about a large number of users, higher requirements must be placed on the care of the data controller in ensuring that no unauthorized access to personal data, and that you, as the data controller, ensure that information about registered persons, including particularly sensitive information, does not come to the knowledge of unauthorized persons.

On this basis, the Danish Data Protection Authority finds that Coop Danmark A/S has not met the requirement for necessary security measures in the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has emphasized that the information has been available in the period 2013 to 2021, and that a company of Coop Danmark A/S's size should have previously been aware that employees may have mistakenly placed personal data on the company's shared drive. It is the opinion of the Danish Data Protection Authority that Coop Danmark A/S should have checked and cleaned up the company's shared drive and introduced relevant security measures at an earlier time.

The Danish Data Protection Authority has also emphasized that the information, i.a. relates to health information, financial information and personal identification number information.

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that Coop Danmark A/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 has noted that Coop Danmark A/S is about to switch to a more secure solution, where e.g. will be better user management and logging.

3.2. Article 33 of the Data Protection Regulation

It follows from the regulation's article 33, subsection 1, that in the event of a breach of personal data security, the data controller must report the breach to the Danish Data Protection Authority without undue delay, and if possible within 72 hours,

unless it is unlikely that the breach of personal data security involves a risk to the rights or freedoms of natural persons.

The Danish Data Protection Authority finds that Coop Danmark A/S has acted in accordance with the data protection regulation, article 33, subsection 1.

In this connection, the Data Protection Authority has emphasized that Coop Danmark A/S became aware of the incident on 9 June 2021, and reported the breach of personal data security to the Data Protection Authority on 12 June 2021. The Data Protection Authority hereby finds that the company has reported the incident in question to The Norwegian Data Protection Authority without undue delay and, if possible, no later than 72 hours after the company became aware of this.

4. Concluding remarks

The Danish Data Protection Authority notes that the Danish Data Protection Authority's decision cannot be appealed to another administrative authority, cf. Section 30 of the Data Protection Act.

However, the Data Protection Authority's decision can be appealed to the courts, cf. § 63 of the Basic Law.

The Norwegian Data Protection Authority expects to publish this decision on the Norwegian Data Protection Authority's website.

The Norwegian Data Protection Authority hereby considers the case closed and will not take any further action in the matter.

[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).