Serious criticism of Salling Group for storing passwords in clear text

Date: 15-07-2022

Decision

Private companies

Serious criticism

Injunction

Reported breach of personal data security

Notification of breach of personal data security

Treatment safety

Password

Unauthorized access

The Danish Data Protection Authority expresses serious criticism of Salling Group for having stored a number of customers' passwords in plain text format in a log file from the grocery group's websites. An error that persisted for more than a year.

Journal number: 2022-441-12449

Summary

The Salling Group uses a common login – the Salling Group profile – so that the username and password can be used on all the services where the Salling Group profile provides access, including Føtex's, Bilkas', Nettos', Salling's and Carl Junior's websites.

In 2021, Salling Group implemented a monitoring tool to register incidents and events - including logins - on the group's websites individually. Due to a human error, the customers' passwords were not encrypted before they were stored in the system's log file when the customers logged in to the website hjem.foetex.dk. As a result, up to 146 internal users in the Salling Group were given technical access to read both usernames and passwords for a number of customers who had logged in on the website.

If this access were used, it would be possible to obtain access to the name, address, email address, telephone number and any masked payment card information and purchase history of a number of Salling Group's customers.

Serious criticism and injunction

Based on the case, the Danish Data Protection Authority expresses serious criticism that Salling Group's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1. on processing security.

The Danish Data Protection Authority has also ordered Salling Group to notify the customers whose passwords have been stored unencrypted in the log for the monitoring tool before 1 August 2022.

Passwords must always be encrypted

Personal data in the form of passwords must always be processed in a way that ensures sufficient security for the personal data in question, including protection against unauthorized access and processing. Passwords must thus be stored at all times in an irreversible encrypted form and in a way that ensures that they are not immediately readable and that it is not possible to recreate the password in a readable format.

Storing passwords in readable format (plain text) in a log file does not meet this requirement. It is the Danish Data Protection Authority's assessment that passwords that can be read in plain text can therefore be subject to abuse, which is why the risk for those registered is high.

Decision

Salling Group A/S (hereafter Salling Group) reported a breach of personal data security on 5 May 2022. The report has the following reference number:

c80d4e631d9e0fe5b57609d8230d7e05508c10a6

This decision replaces the Danish Data Protection Authority's decision of 7 July 2022, as the Danish Data Protection Authority has, at the request of Salling Group, corrected a number of factual information and reassessed the decision.

1. Case presentation

It appears from the case that in 2021 Salling Group implemented a service for recording incidents and events in connection with customers' access to a number of Salling Group's websites. By mistake, the customers' passwords were not encrypted before they were stored in the log for the monitoring tool that registered incidents and events on the website hjem.foetex.dk, which is why up to 146 internal users in the Salling Group had technical access to read usernames and passwords for a number customers who logged in to the website hjem.foetex.dk.

2. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Salling Group'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 instructs Salling Group to notify, before 1 August 2022, the customers whose passwords have been stored unencrypted in the log for the monitoring tool and thus have been accessible to up to 146 of Salling Group's employees. The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter e.

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

3. Salling Group's comments

Salling Group has stated in the notification to the Danish Data Protection Authority of 6 May 2022, and subsequent consultation and telephone follow-up, that in 2021 Salling Group implemented a system for use by customers to access a number of Salling Group's websites individually. From 7 January 2021, Salling Group employees tested the entire flow in the system from purchasing to delivery at the home address. Public access to the service was granted on 1 February 2021, after which customers were given access to log in via the service on the website hjem.foetex.dk and the other services to which the Salling Group profile provides access, including Føtex, Bilka, Netto, Salling and Carl Junior. Customers could then make purchases on any of these pages.

On 6 May 2022, the Salling Group found that customers' usernames and unencrypted passwords were stored in the system's log file for the website hjem.foetex.dk by mistake, after which the system was taken out of service.

An investigation showed that, by mistake, an employee had not switched on masking/encryption of passwords in the monitoring tool that logged incidents and events on the website hjem.foetex.dk, whereby customers' usernames and passwords from this system were stored in plain text in the log for one month at a time. The information has not been accessed in any way via the system's front end. The error was corrected, the unencrypted log data was deleted and the system was put back into operation.

The Salling Group points out that only 146 people within the Salling Group have had technical access to the log files in question; of these, it is estimated that there were only 5 who had the necessary technical knowledge to be able to search for the information. Salling Group states that these 5 employees are all internal employees, are subject to Salling Group's

instructions and otherwise employed in positions of a confidential nature, which is why Salling Group considers that the risk for those registered is not high.

Salling Group states in the response to the hearing that if an unauthorized person gained access to the username and password, that person would be able to log on to other Sallings Group services where the Salling Group profile provides access - of course depending on which services the username and password in question were valid for - and thereby gaining access to name, address, email address, telephone number, and any masked card information and purchase history. There is also a theoretical probability that the customer may have used the same email address and password for other services with other data controllers, and unauthorized access to the unencrypted passwords could thus hypothetically give access to e.g. social media, streaming services, email accounts or the like.

4. Reason for the Data Protection Authority's decision

The Danish Data Protection Authority assumes from Salling Group's notification of 6 May 2022, the subsequent consultation response and telephone follow-up that Salling Group has stored a number of the company's customers' passwords in the log for Salling Group's monitoring tool, without these being encrypted, whereby up to 146 employees had access to usernames and passwords for a number of customers. If this access were used, it would be possible to gain access to the name, address, email address, telephone number, as well as any masked payment card information and purchase history for a number of Salling Group's customers.

The Danish Data Protection Authority is of the opinion that personal data in the form of passwords must be processed in a way that ensures sufficient security for the personal data in question, including protection against unauthorized access and processing. Passwords must therefore be stored in irreversible encrypted form at all times and in a way that ensures that these are not immediately readable and that it is not possible to recreate the password in a readable format. Storing passwords in a readable format in a log file does not, in the opinion of the supervisory authority, meet the requirements of Article 32, paragraph 1 of the Data Protection Regulation. 1.

The Danish Data Protection Authority is of the opinion that passwords that can be read or stored in clear text can be subject to abuse. In addition, the Danish Data Protection Authority is of the opinion that it is a known risk scenario that the compromise of trading platforms and logging information on these are often made the subject of external attacks or that internal access is used unjustifiably. It is therefore the Danish Data Protection Authority's assessment that this risk for the data subjects is

relatively high.

4.1. 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 confidential information about a large number of users, higher requirements must be placed on the care of the data controller in ensuring that there is no unauthorized access to personal data, that a procedure is carried out for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security and that, as the data controller, you ensure that information about registered persons, including confidential information, does not come to the knowledge of unauthorized persons.

4.2. Decision

Based on the above, the Danish Data Protection Authority finds that Salling Group - by collecting and storing customers' passwords in the log for the company's monitoring tool without these being encrypted - has not taken appropriate organizational and technical measures to ensure a level of security that suits the risks that are in the company's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

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

When choosing a response, the Danish Data Protection Authority emphasized the fact that there are a large number of customers whose passwords were stored and were available in a readable format, which could have serious consequences for the customers if their personal data fell into unauthorized hands.

Salling Group has informed the Danish Data Protection Authority that the error has been corrected so that unencrypted passwords are no longer stored in the monitoring tool's log. Furthermore, Salling Group has definitively deleted all

backward-looking user data from the log files.

5. Injunction

The Danish Data Protection Authority finds grounds to notify Salling Group of an order to notify the customers whose passwords have been stored unencrypted in the log of the company's monitoring tool and thus have been accessible to up to 146 of Salling Group's employees. The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter e.

The Danish Data Protection Authority assumes that a number of customers' passwords have been stored in clear text and that up to 146 employees had access to the information.

Regardless of the fact that the log only went back 30 days, the Danish Data Protection Authority finds that – given that access rights were granted to up to 146 users and that the information contained, among other things, name, address, email address, telephone number, and any masked card information and purchase history for a number of customers – considered to the known risk scenarios, means that there is probably a high risk to the rights and freedoms of the data subjects. The Danish Data Protection Authority therefore considers that the data subjects must be notified in accordance with Article 34 of the Data Protection Regulation.

The deadline for compliance with the order is 1 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 e.

[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).