The Danish Data Protection Authority has expressed serious criticism that Designbysi has not met the requirement for necessary security measures in the GDPR

Date: 22-06-2022

Decision

Private companies

Serious criticism

Reported breach of personal data security

Treatment safety

Hacking and others

Password

Unauthorized access

Designbysi was exposed to a hacker attack, where unauthorized persons collected customers' card details. Prior to the incident, multifactor login was not introduced for users who had access to change the payment script.

Journal number: 2021-441-9489

Summary

The Danish Data Protection Authority has made a decision in a case where Designbysi ApS has reported a breach of personal data security.

Designbysi was exposed to a hacker attack, where an unauthorized person inserted a JavaScript on Designbysi's webshop to collect their customers' card information.

Before the incident, Designbysi had not introduced multi-factor login for the users who had access to change the payment script.

On this basis, the Danish Data Protection Authority found grounds for issuing serious criticism of Designbysi.

1. Decision

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

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

2. Case presentation

On 25 June 2021, Designbysi reported a breach of personal data security to the Danish Data Protection Authority.

It appears from the notification that external parties had inserted an unauthorized JavaScript on Designbysi's webshop in order to collect their customers' card information. The JavaScript resulted in customers receiving an error message in connection with their purchase, after which they were asked to enter their card details once more.

Designbysi has stated that on 22 June 2021 they received an email from Nets regarding the breach of personal data security, and Designbysi contacted the Data Processor immediately afterwards. On the same day, the unauthorized JavaScript was disabled on the webshop.

It appears from the statement from the Data Processor that, on the basis of logs, the Data Processor could conclude that the attack was only seen actively on 23 April 2021.

It also appears from the statement from the Data Processor that the attack was probably carried out by using stolen/guessed login information for the specific webshop. The data processor based this conclusion on the fact that only Designbysi's webshop had the unauthorized JavaScript, which points to a specific reason for the attack.

The data processor has stated that it is not possible to state exactly how many and which cards have been affected. But the Data Processor suspects that the attack may have potentially affected everyone who shopped at designbysi.dk between 26 April 2021 and 22 June 2021, both days inclusive.

This will also include cardholders who gave up after the error message, and thus there is no concrete information about them.

Designbysi has stated that it could potentially be all X-number of customers who have shopped on the Danish site during the period that are affected. On 28 June 2021, Designbysi sent out an email to all affected customers regarding the breach of personal data security and recommended that customers contact their bank.

Designbysi has also stated that on 22 June 2021 they have introduced two-factor authentication for all six of their users, as well as written passwords. All six people, three of whom are owners, have been informed to be careful with any harmful links in emails. All Designbysi's computers have been cleaned and checked for possible intruders, but nothing has been found.

In addition, Designbysi has asked the Data Processor to remove Designbysi's option to change the payment script. In this connection, Designbysi has stated that this – at the time of the response on 29 July 2021 – was not possible, but something

Designbysi would push for.

Designbysi has stated that the Data Processor has replied: "The incident occurred when a 3rd party gained access to the webshop's control panel by knowing the username and password. The webshop system itself has had no security holes.”

Subsequently, the Data Processor has made Designbysi aware of two-factor authentication, to which the Data Processor has given Designbysi access, and which Designbysi has archived on all logins.

The data processor has informed Designbysi that the data processor does not verify code or changes that the customer himself installs on the webshop. It is the responsibility of the webshop owner to verify and check the code and the changes he makes to his webshop.

In this connection, Designbysi has stated that they do not agree as a customer. Designbysi does not see how they would be able to detect the problem themselves, or decipher different JavaScripts in a setup.

3. Reason for the Data Protection Authority's decision

Based on the information provided to the case, the Danish Data Protection Authority cannot ascertain which weakness at Designbysi the unauthorized party has exploited.

Based on the information provided by Designbysi and the Data Processor, the Data Protection Authority assumes that Designbysi only introduced two-factor authentication for administrative rights to the webshop and the domain after the incident.

The Danish Data Protection Authority also assumes, on the basis of the information provided, that the login information of six employees gave access to changes in the payment script.

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 login information that gives access to payment information or the possibility to change the payment script must be secured against hackers being able to access the information with a unique username and password alone , eg. from a phishing attack. It is therefore the Danish Data Protection Authority's assessment that it is an appropriate security measure to implement multi-factor authentication on such login information. In addition, the authority is of the opinion that access to payment modules and change rights to the domain should generally be limited to a specially named account that is only used for this purpose and a suitable complex password with simultaneous multi-factor login, this to reduce the possibility that those accounts employees use on a daily basis, an attack on their daily communication compromises the payment service and the access security of the root domain.

The Danish Data Protection Authority finds, on the basis of the above, that Designbysi – by failing to carry out such double verification – has not taken appropriate organizational and technical measures to ensure a level of security that is suitable for the risks involved in Designbysi's processing of personal data, cf. the data protection regulation's 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 Designbysi's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

In choosing to react in a stricter direction, the Danish Data Protection Authority has emphasized that the lack of security measures made it possible for the hackers to gain access to payment information about Designbysi's customers, which could potentially cause financial damage to the affected customers.

The Danish Data Protection Authority has noted that, in continuation of the case, Designbysi has introduced two-factor authentication for all six of their users, as well as written passwords.

For guidance on strong passwords, the Danish Data Protection Authority also refers to the Center for Cyber Security's password guidance[2] or NIST 800-63-3.

[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] https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-vejledning-passwordsikkerd-2020.pdf