Criticism of [jo:ga] ApS's lack of processing security

Date: 22-10-2021

Decision

Private companies

Criticism

Injunction

Complaint

Treatment safety

Password

The Danish Data Protection Authority has expressed criticism that Joga did not have adequate security. The Danish Data Protection Authority also ordered the company to bring the processing of personal data into line with the data protection regulation.

Journal number: 2020-31-4326.

Summary

The Danish Data Protection Authority has made a decision in a case where a member of Joga complained that the password for logging in to Joga's site and app was the complainant's date of birth, and that there were no restrictions on the number of login attempts.

The Danish Data Protection Authority found that Joga – by not having made restrictions on unsuccessful login attempts, and by using the members' date of birth as a password that could not be changed – had not taken appropriate security measures.

In the assessment, the Danish Data Protection Authority emphasized that known or easily accessible information, e.g. a date of birth, should only be used as an initial password, which must subsequently be changed.

The Norwegian Data Protection Authority also emphasized that the insufficient security measures made it possible for unauthorized persons to gain access to the members' personal data.

Against this background, the Danish Data Protection Authority expressed criticism that Joga's processing of personal data had not taken place in accordance with the rules on processing security.

The Norwegian Data Protection Authority also ordered Joga to bring the processing of personal data in line with the data

protection rules, by forcing Joga's current and new members to change their passwords to a necessary secure password upon first login, where requirements are placed on the complexity of the code.

Joga has stated on 13 October 2021 that they have complied with the order.

Decision: The Danish Data Protection Authority hereby returns to the case where […] (hereafter complainant) on [date] 2020 has complained that [jo:ga] ApS (hereafter Joga) does not process information about her sufficiently securely.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that Joga'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 grounds to notify Joga of an order to bring the processing of personal data in line with the data protection regulation's article 32, subsection 1, in that Joga's current and new members are forced to change their passwords to a necessary secure password upon first login, where requirements are made for the entropy of the code.

The order is announced pursuant to Article 58 subsection of the Data Protection Regulation. 2, letter d.

The deadline for compliance with the order is 7 October 2021. The 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.

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 case that the complainant is a customer of Joga and that her membership number is "jo" followed by seven numbers. The complainant's password for logging in to Joga's website and app was originally the complainant's date of birth.

In January 2020, the complainant contacted Sport Solution about a possible security flaw in the booking and membership system that the company sells. The complainant stated that Sport Solutions' customers were bothered by consecutive membership numbers and that the password was always the member's date of birth. The complainant further stated that she could ask for combinations of membership number and password as many times as she wanted.

Sport Solution replied that Joga is one of their customers and that it is the customer's own decision which safety standards are set up. Sport Solution stated that they would contact Joga and advised complainants to do the same.

The complainant then contacted Crossfit Copenhagen (now Arca), who stated that Arca was in dialogue with the provider of the system.

In August 2020, the complainant informed Sport Solution that Arca had informed her that they were jointly making improvements to the set-up, but that the complainant could not see that they had made any safety improvements since her inquiry in January 2020.

2.1. Joga's remarks

On 19 January 2021, Joga made a statement in the matter. Joga has claimed that some time ago they introduced a limitation on the number of login attempts.

Joga has stated that it is possible to change the password by writing to the company. Joga is also in the process of implementing that you can change your password directly in the app.

In addition, Joga has stated that when you log into the booking app, there is no personally sensitive information. There is only first name and training history.

On 4 May 2021, Joga has additionally stated that Joga has implemented that you can change your password. In addition, Joga will implement a security measure which means that after five unsuccessful login attempts you will be locked out for one hour and after 10 times you must write to Joga to be unlocked again.

2.2. Complainant's comments

The complainant has stated that the password is systematically the date of birth for all customers of Joga, and that you cannot change your password via Joga.dk. You can, on the other hand, change your password via booking.sport-solutions.dk/login, but the complainant had to figure that out himself. Neither Joga nor Sport Solution had informed about this possibility.

The complainant has also stated that the problem with the described system in login information is that Joga has no restrictions on the number of incorrect login attempts. The complainant has therefore been able to write a very simple script that finds other private customers' valid login information by trying to log in with membership numbers and passwords that follow the described system. In this connection, the complainant has stated that the system does not reset passwords or detect that she is using a script. The complainant has stated that the script is slow and that it only finds login information for one

private customer. That customer was originally the complainant himself, but the complainant has also tried with the login details of an acquaintance, who has given consent for the complainant to use the information as evidence to the Norwegian Data Protection Authority.

Following Joga's original statement, the complainant stated that she was unsure whether a limitation on the number of login attempts had actually been introduced, and if so, whether the limitation was sufficient, since with a minor change to the complainant's script it was possible to make over 300 login attempts before the code guessed complainant's known date of birth, which is 23 December.

3. Reason for the Data Protection Authority's decision

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 the data controller must ensure that information about registered persons does not come to the knowledge of unauthorized persons.

The Danish Data Protection Authority finds that Joga - by not having implemented restrictions on unsuccessful login attempts, and by using the members' date of birth as a permanent password - has not taken appropriate organizational and technical measures to ensure a level of security suitable for the risks associated with Joga's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has emphasized that known or easily accessible information should only be used as an initial one-time identifier, and that the insufficient security measures make it possible for unauthorized persons to gain access to members' personal data, e.g. through a so-called brute force attack, or by acquiring information about a member.

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that Joga'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 also finds grounds to notify Joga of an order to bring the processing of personal data in line with the data protection regulation's article 32, subsection 1, in that Joga's current and new members are forced to change their passwords to a necessary secure password upon first login, where requirements are made for the entropy of the code. The order is announced pursuant to Article 58 subsection of the Data Protection Regulation. 2, letter d.

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

The Danish Data Protection Authority has noted that Joga, in continuation of this case, has implemented that after five unsuccessful login attempts you will be locked for one hour, and that after 10 attempts you must write to Joga to be unlocked again.

[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).

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