Security breach at the ZOO

Date: 18-11-2020

Decision

Private companies

The Danish Data Protection Agency expresses serious criticism that, among other things, was far too easy to gain unauthorized access to personal information about the annual card holders at the Zoo in Copenhagen.

Journal number: 2020-441-4364

Summary

On the basis of a reported breach of personal data security at the Copenhagen Zoo (ZOO), the Danish Data Protection Agency is now expressing serious criticism. The technical setup of the login page for annual card holders made it easy for unauthorized persons to access other people's personal information. In addition, there were inaccuracies in the communication in connection with the breach of personal data security.

The ZOO has been ordered to rectify the incomplete information to all data subjects and an order to inform the data subjects of the breach in cases where there is a high risk.

The decision was made because the Danish Data Protection Agency found that it was not a question of appropriate security, as it had been too easy to obtain unauthorized access to annual cardholders' personal information. Login for annual card holders was a combination of two numerical values without limitation in the number of login attempts.

The criticism is further that the ZOO's description to the Danish Data Protection Agency and in the communication with the data subjects of the measures taken by the ZOO to deal with the breach was not correct in relation to what the ZOO actually did and the Data Inspectorate's perception of the risk scenarios.

In addition, the Danish Data Protection Agency found that the ZOO had not notified the data subjects (annual cardholders) for whom there was a high risk, and that the information otherwise provided was not accurate and did not indicate probable consequences, risk scenarios or the duration of the breach. Therefore, the communication did not help the data subjects to assess what precautions they might need to take to protect themselves.

Decision

The Danish Data Protection Agency hereby returns to the case where the Zoo in Copenhagen (hereinafter "Zoo") on 3 January

2020 reported a breach of personal data security to the Authority.

Decision

Following an examination of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that Zoo's processing of personal data has not taken place in accordance with the rules in Articles 32, 33, 34 and 5 (1) of the Data Protection Regulation [1]. 1, letter a.

The Danish Data Protection Agency also finds grounds for issuing an order to Zoo to notify all data subjects where there is a high risk of their rights. The injunction is granted pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter e.

The content of the notification must comply with the requirements of Article 34 (1) of the Data Protection Regulation. Describe in such a clear language the nature of the breach of personal data security and contain at least the information and measures referred to in Article 33 (2). 3, letters b, c and d.

The Danish Data Protection Agency finds further grounds for issuing an order to Zoo to bring the processing of personal data in accordance with Article 5 (1) of the Data Protection Regulation. 1, letter a, by correcting the previously given information so that it reflects the assessments of the risk that the Danish Data Protection Agency has accounted for in this decision, this in relation to all affected data subjects. The injunction is granted pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d.

The deadline for compliance with the orders is 1 December 2020. The Danish Data Protection Agency must request by the same date to receive a confirmation that the orders have been complied with, together with an anonymised version of the notification and the manner in which this has been given.

According to the Data Protection Act [2] § 41, para. 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter e.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. Case presentation

It appears from the notification of the breach to the Danish Data Protection Agency that a person (hereinafter the "software engineer") on 2 January 2020 - via a self-developed script - acquired access to annual card holders' log-in information (username and associated password). The software engineer informed Zoo about the vulnerability in Zoo's login, which made

this possible.

The vulnerability in Zoo's log-in allowed us to try to access a valid log-in (username and password), which in turn gave unauthorized access to the annual cardholder's card number, name, address and e-mail. At this time, the zoo had approx. 140,000 annual card holders registered.

3. Zoos remarks

Zoo has stated that the vulnerability in the log-in used gave access to the annual cardholder's 8-digit membership number (username), the 4-digit password, card number, name, address and e-mail. The latter is understood by the Danish Data Protection Agency as knowledge of the annual card holder's "e-mail address".

Zoo denies that there were access to phone numbers and pictures, which according to Zoo is alleged by the software engineer.

According to the Zoo, the password requirement was a four-digit number, and no automatically generated passwords have been used.

Asked about measures against "brute-force attacks" on log-in (login information is found by trying to find a valid username / password combination), Zoo has stated that information is sent encrypted between client and server. Zoo has explained that the IT solution did not automatically block many unsuccessful log-in attempts, just as it was not logged.

It appears from the case that the software engineer had gained access to log-in information (username and password), which enabled him to log in as annual card holders, but he has not used this log-in information.

The zoo implemented the following measures in the wake of the breach of personal data security: (1) the "I am not a robot" function, which ensures that a program can not cheat the system, and (2) a function that, after three erroneous log-in attempts blocks log-in for one hour.

The zoo announced that a new log-in feature was created, in which the Center For Cyber Security's password recommendations were implemented. In this connection, all annual card holders were forced to change their password.

Based on a study of web page views, the zoo has assessed that there have been no fluctuations in relation to the normal number of page views, and on that basis has assessed that it is unlikely that personally identifiable data has been exposed to unauthorized persons. It is Zoo's conclusion that there have been no other attacks of the nature of those carried out by the software engineer. The zoo justifies this with especially ongoing monitoring of logs. When asked, Zoo stated that the log does

not record information on whether many unsuccessful login attempts were made from the same IP address, or many unsuccessful log-in attempts with the same username (member number) and different passwords - throughout the period 25 May 2018 to 2 January 2020.

The zoo has not been able to state how many of the approx. 140,000 annual card holders potentially affected by the breach. The zoo stated that the software engineer said he could access information for any (a sample) of the annual card holders. The number of potentially affected can thus not be stated. Zoo is not in possession of the script used by the software engineer.

The zoo has not been able to state how long it has been possible to exploit the weaknesses in the log-in to gain unauthorized access to the annual cardholders' personal information. This is due to the fact that the website is constantly updated.

When asked whether Zoo has considered the possibility of secret addresses among the personal data concerned, and whether Zoo knows for sure that there are no secret addresses in between, Zoo answers that it has been included in the considerations and that none of Zoo's annual card holders have given Zoo notice of, name and address protection.

Notification of the data subjects

Upon notification of the breach on 3 January 2020, the Zoo stated that there had been partial notification of the data subjects on the same day. Notification had been made via email and website. The content of the notification is described, but it does not include a description of the likely consequences of the breach of personal data security, or an approx. indication of the period during which the breach lasted. However, the notification contained a link and the text "Via the link below you can read more about the most frequently asked questions", but this link was not included in the notification to the Danish Data Protection Agency.

At a hearing, the Zoo stated that the notification was sent to all approx. 140,000 annual card holders on January 3, 2020.

The Danish Data Protection Agency informed the Zoo that the Authority had knowledge of annual card holders who had not received the notification in question per. e-mail, even if they had an e-mail address registered with the Zoo. Against this background, Zoo stated that an extract of e-mail addresses had been made from the system, and persons without a registered e-mail address have been notified through the news that was on Zoo's website for some time (the front page of the website). Other factors, such as the annual cardholder's opt-out of news from the Zoo, could also have an effect on whether these persons were notified per. e-mail - this could not be definitively clarified, as the extraction of e-mail addresses was made by an employee who was on leave. The extract indicates 23,662 unique e-mail addresses, as duplicates are sorted out so that if e.g.

several people in a family have an annual card, but they have a common e-mail address, this will only appear once in the extract.

A kind of test was made on 27 May 2020, where an extract of active annual card holders with registered e-mail address - including those who have opted out of news from the Zoo - gave 40,257 e-mail addresses.

When Zoo was asked about the reason for the non-indication of consequences in the notification of the data subjects, Zoo referred, among other things, to the fact that there are no indications for exposure of data to unauthorized persons and that the risk to natural persons' rights and freedoms is therefore assessed as minimal / non-existent, and that this is only ordinary personal information.

In response to the third hearing, the Danish Data Protection Agency received the link that was included in the notification. The website linked to states, among other things, that "the Software Engineer has only pointed out the potential vulnerability that has now been closed. Your membership information has therefore not been shared or otherwise compromised."

The zoo has further stated that the public has been informed of the incident, as Politikken, TV2 Lorry and B.T. in collaboration with the software engineer brought the story.

4. Justification for the Danish Data Protection Agency's decision

3.1. Article 32 of the Data Protection Regulation

Establishment of appropriate level of security

In assessing the appropriate level of security, particular consideration shall be given to the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise; dealt with in accordance with Article 32 (2). 2.

Based on the descriptions of Zoo's log-in, the Danish Data Protection Agency finds that - with or without automation - it must be considered to have been relatively easy to obtain unauthorized access to the annual cardholders' personal information. This is based on a compilation of the following conditions in the affected log-in.

In addition to a four-digit password generally calling for the use of bad codes, such as the annual cardholder's postcode, parts of social security number or similar, there are a maximum of 10,000 combinations. When this is combined with the username being an 8-digit number and no protection against automation of log-in attempts was implemented, and when furthermore there was no restriction of unsuccessful log-in attempts from the same IP address or combinations by the same username with

different passwords (or vice versa), it becomes possible to quickly access the personal cardholders' personal information. The Authority finds that there should have been a restriction on e.g. 3-5 unsuccessful access attempts with the same username or from the same IP address (with changing usernames).

Against this background, the Danish Data Protection Agency finds that Zoo has not complied with Article 32 (1) of the Data Protection Regulation. 1, as an appropriate level of security has not been implemented taking into account the risks posed by the processing of the annual cardholders' personal data.

The Danish Data Protection Agency has taken note of Zoo's information that the Center For Cyber Security's recommendations regarding passwords have now been implemented.

Regular evaluation of measures

Article 32 (1) of the Data Protection Regulation Article 1 (1) (d) states that in order to ensure a level of security appropriate to the risks involved in the processing of personal data, it may be appropriate to have a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure treatment safety.

Given that the vulnerable log-in is an IT solution that controls access to personal information for approx. 140,000 people, the Danish Data Protection Agency is of the opinion that there should have been a procedure that ensures regular assessment of the effectiveness of the measures in the Zoo's log-in that are to secure the personal data against unauthorized or illegal processing.

3.2. Article 33 of the Data Protection Regulation

When notifying the Data Inspectorate of the breach, the data controller must describe the measures that the data controller has taken or proposes to take to deal with the breach of personal data security, including, if applicable, measures to limit its possible harmful effects, cf. Article 33 (1). Notification of the data subject of the breach in accordance with Article 34 is - when this is relevant - an example of such a measure, as the data subject may can use the information to limit the harmful effects.

In connection with the notification of the case and in the additional material sent for notification, the Zoo is informed that notification had been sent to all 140,000 annual card holders.

The Danish Data Protection Agency states that it later stated in the case that notification had been sent to 26,662 unique e-mail addresses, and that it had been Zoo's opinion that the data subjects who did not receive this e-mail were notified via the website and through press coverage of the case.

At the time of the initial notification of the breach to the Danish Data Protection Agency, the said distinction regarding the nature of the notification did not appear.

It is the opinion of the Danish Data Protection Agency that in order to ensure the rights of the data subjects, it is essential that the information in the notification does not appear in such a way that measures are stated that have not actually been implemented or do not reflect the number of people affected. so it is unclear who is covered by what measures and when.

Against this background, the Danish Data Protection Agency is of the opinion that Zoo's description, cf. Article 33, subsection 3, letter d of the measures taken to deal with the breach, was not fair in relation to what the Zoo actually did and thus has not lived up to the description requirement in Article 33, para. 3.

3.3. Article 34 of the Data Protection Regulation and Article 5 (1) 1, letter a.

Assessment of the risks that the breach poses to the data subjects' rights

Where a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the controller shall without undue delay notify the data subject of the breach of personal data security pursuant to Article 34 (1).

Therefore, the Zoo had to assess the risks that the breach entailed for the annual card holders.

The Danish Data Protection Agency assumes that Zoo's conclusion that there has been no abuse of the log-in vulnerability is based on a study of log files from the tool Analytics, which shows that in the period 25 May 2018 to 3 January 2020, there have been 12468 sessions in total and member data has been accessed 44328 times. Furthermore, Zoo emphasizes that no annual card holders have reported unauthorized changes to their data.

It is the Data Inspectorate's assessment that the mentioned log files primarily focus on the ordinary user behavior, and in the Authority's view are not an expression of an investigation that is optimized to detect possible abuse. The Danish Data Protection Agency is of the opinion that even in situations where the usage pattern occurs normally, there may be an abuse situation. It is therefore not possible - on this background alone - to conclude that the potential opportunity for unauthorized access has not been exploited. Unauthorized access to information can occur in a way that does not attract attention because it resembles normal data traffic, and thus is not detected by an investigation such as the one described by the Zoo.

It is the Data Inspectorate's assessment that information on name combined with e-mail address and card number on the annual card constitutes a risk for the registered persons. The information can e.g. is used to send e-mails in which someone pretends to be a Zoo, thereby spreading computer viruses and so-called "ransomware", or luring other information out of the

victims, e.g. credit card information - called "phishing". The registrants can be more easily cheated because they assume that the information about their e-mail address combined with the correct card number is only known by Zoo.

At the same time, in the Authority's view, this is an example of how the data subjects can be helped to protect themselves by being informed of the breach and its probable consequences. This, incidentally, regardless of whether the data controller is obliged to do so or not.

According to the information in the case, the zoo did not perceive the situation as covered by the notification requirement, cf. Article 34 (1). 1, Zoo has, however, notwithstanding this, informed the data subjects about the incident in several ways.

In the opinion of the Danish Data Protection Agency, secret / protected addresses constitute personal data that must be subject to a high degree of confidentiality, as an unintentional exposure of such information can potentially have serious consequences for the data subjects' rights.

The Danish Data Protection Agency assumes that, given the high number of registered approx. 140,000, will be registered with secret or protected addresses among these. The Authority is of the opinion that, at least for these data subjects, by exposing their address, there will be a high risk to the rights of the persons concerned, especially given the consequences such exposure may have.

The fact that the data subjects themselves did not state their address as secret may - also given that there was no dedicated way of marking this attribute - not lead to a different result.

The Danish Data Protection Agency does not consider that an adequate assessment has been carried out in accordance with Article 34 (1) of the Data Protection Regulation. 1, of the risk for the data subjects' rights, and that at least for the said data subjects there is a high risk for their rights. The Danish Data Protection Agency has emphasized the following in particular.

Extent / duration of the fracture

The zoo has not been able to demonstrate that anyone other than the software engineer has taken advantage of the opportunity to gain unauthorized access. Therefore, the Danish Data Protection Agency assumes that all approx. 140,000 annual card holders could potentially be compromised.

When the Zoo is unable to indicate how long the log-in has been vulnerable due to continuous updating of the site, it implies a lack of knowledge about the extent of the breach. It also means that the Zoo cannot know which annual card holders are affected, as new annual card holders may be registered both before and after the vulnerability arose.

It is clear from the preamble 86 of the Data Protection Regulation that the data controller's notification of the data subject of a breach of personal data security is made with a view to enabling him or her to take the necessary measures, and the notification should include recommendations to the natural person concerned. limit the possible harmful effects.

When the Zoo does not know and cannot inform about the duration of the breach, it gives the data subjects less than optimal opportunities to take the necessary precautions. It can e.g. be the case if the registered personal data has changed along the way over a period over the occurrence of the breach.

If e.g. annual card holders have changed address recently, it is difficult for them to assess whether the breach has been able to reveal the previous address or not. Previous addresses can e.g. indicate a former cohabitant, or it could be an address there revealing residence in a specialized institution or under the penitentiary.

According to what the Zoo stated in the case, the Danish Data Protection Agency assumes that the Zoo cannot document how long the breach has lasted and that this matter was not included in the notification by the data subjects.

Content and form of the notification

In relation to the content and form of the notification, the Danish Data Protection Agency finds that it does not meet the requirements of Article 34 of the Data Protection Ordinance. In this connection, the Danish Data Protection Agency has emphasized the following.

In cases where the breach of personal data security has a longer period of time, the Danish Data Protection Agency is of the opinion that the use of an unverified previously informed e-mail is not necessarily adequate, especially if it has been a long time since the original registration took place and the vulnerability has stood on for a period of unknown length, as the annual cardholders may have changed their e-mail accounts during this period.

The notification of the data subjects, which according to the Zoo has taken place by a combination of e-mail, the Zoo's website and media coverage, does not contain a description of the probable consequences of the breach, cf. Article 33 (1). Article 34 (3) (c) 2.

The website also states that the breach did not result in compromise of member information, and the situation is described as a "potential vulnerability", which may give the reader the impression that there has been no real possibility of unauthorized access to personal information. The Data Protection Agency does not find that Zoo has correctly described the breach of personal data security, especially when it is the Authority's view that, since lack of protection against "brute force" attacks, the

limited log information, and lack of knowledge about how long the vulnerability has existed.

The Danish Data Protection Agency thus finds that Zoo has provided information to the data subjects which is incomplete and accurate, which does not state the probable consequences or the duration of the breach, and which therefore does not help the data subjects to assess what precautions they may have to take to protect themselves. The Data Protection Supervisor therefore finds that the data subjects have not been notified in accordance with the content of Article 34.

The Danish Data Protection Agency assesses that the breach of personal data security constitutes a high risk for, among others, the registered persons with a secret / protected address, which is why the Authority finds that at least these data subjects must be notified, cf. Article 34 (1). 4.

Furthermore, the Data Inspectorate is of the opinion that the other data subjects have been exposed to an increased concrete risk through the information published by the Zoo itself (the website text), as these data subjects could mistakenly believe that their information was not in any danger of being compromised. It follows from the principle of Article 5 (1) of the Data Protection Regulation 1, letter a, that the principle of fair and transparent processing dictates that incorrectly or insufficiently given information is corrected, regardless of whether the risk to the data subjects' rights may be high or not.

In view of this, the Danish Data Protection Agency finds that there is also a violation of Article 5 (1). 1, letter a, and that this must be brought in accordance with the regulation, in that, in accordance with the data subjects, these matters are rectified by notification.

If the Zoo finds that it is not possible or requires a disproportionate effort to make an individual notification of the data subjects, the Danish Data Protection Agency finds that notification can be made by public announcement or similar measure, if this is done in a way that ensures that they data subjects shall be notified in a similarly effective manner in accordance with Article 34 (2) of the Data Protection Regulation. 3, letter c.

3.3. Summary

The Danish Data Protection Agency finds reason to express serious criticism that Zoo's processing of personal data has not complied with Article 32 (1) of the Data Protection Regulation. 1 and 2, Article 33, para. Article 34 (3) (d) 1 and 2, and Article 5, para. 1, letter a. The Danish Data Protection Agency has hereby emphasized the following as aggravating circumstances:

That there is a large number of registered.

That the combination of a password consisting of four numbers, and without protection against automation of endless attempts

at log-in, has meant insufficient protection of personal data.

Zoo's lack of knowledge about how the log-in solution has worked in the past with the consequent limited opportunity to assess risks of the breach.

That the Zoo has assumed that there were no protected addresses among the registered information, solely because this was not disclosed by the annual card holders themselves.

That Zoo's notification of the data subjects was deficient, and the content not truthful.

That Zoo's description of measures related to the breach was not true.

The Danish Data Protection Agency also finds grounds for issuing an injunction pursuant to Article 58 (1) of the Data Protection Regulation [3]. 2, letter e, to notify all data subjects where there is a high risk of their rights, for the other data subjects, the Danish Data Protection Agency notifies pursuant to Article 58 (1) of the Data Protection Regulation. In accordance with Article 5 (2) (d) of the Zoo, to bring the processing of personal data into line with Article 5 (2) of the Data Protection Regulation. 1, letter a, by correcting the previously given information so that it reflects the assessments of the risk that the Danish Data Protection Agency has accounted for in this decision.

The Data Protection Authority must state that the Authority will consider both orders to be fulfilled if all data subjects receive the information mentioned in Article 34 (1). 2, possibly on the one in Article 34, para. 3, letter c, mentioned manner.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act)

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).