Insufficient security measures at T. Hansen

Date: 15-11-2021

Decision

Private companies

Criticism

Injunction

Complaint

Notification of breach of personal data security

Treatment safety

Password

Unauthorized access

The Danish Data Protection Authority has criticized the fact that customer profiles at T. Hansen have not had appropriate security measures - and has given the company an order to encrypt the customers' passwords.

Journal number: 2021-31-4596.

Summary

A customer of T. Hansen Gruppen A/S has complained to the Norwegian Data Protection Authority that the company has not had adequate security measures.

The complainant in the case had a customer profile where the customer number was identical to the complainant's telephone number. The complainant changed his telephone number at one point, while an unauthorized person took over the complainant's previous telephone number. When the unauthorized person then made a purchase from T. Hansen, the complainant's and the person's information were combined on the complainant's customer profile. For a period of time, the unauthorized person had access to the complainant's information and access to receive the complainant's password in plain text.

The Danish Data Protection Authority expressed criticism that T. Hansen has not met the requirements of the data protection regulation regarding appropriate security measures and notification of breaches of personal data security.

The Danish Data Protection Authority justified this by saying that T. Hansen had not taken into account when developing his

system that customers' information could risk being combined, for example as a result of a telephone number being transferred from one person to another.

The Danish Data Protection Authority is of the opinion that the reuse of telephone numbers is a normal and expected scenario, which is why it should have been included in the determination of the relevant security measures.

The Danish Data Protection Authority has also emphasized that T. Hansen has stored the user's self-selected passwords in clear text in its system without a recognized algorithm for an irreversible encryption thereof, and that T. Hansen has had a function where users have been able to receive passwords in clear text to the user's specified e-mail address upon request, notwithstanding that T. Hansen has not carried out a risk assessment.

On that basis, the Danish Data Protection Authority has given T. Hansen an order to use a recognized algorithm for encryption (e.g. hashing) of all passwords, so that these are not stored or can be recovered in clear text. T. Hansen has stated on 4 November 2021 that they have complied with the order.

1. Decision

After a review of the case, the Data Protection Authority finds that there is a basis for expressing criticism that T. Hansen Gruppen 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, and Article 33, subsection 1.

The Danish Data Protection Authority also finds grounds to notify T. Hansen Gruppen A/S of an order to - to the extent that T. Hansen Gruppen A/S still stores passwords in plain text - use a recognized algorithm for encryption (e.g. hashing) of all passwords , so that these are not stored or can be restored in plain text.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d. It should be noted in this connection that failure to comply with an order from the Data Protection Authority can be punished with a fine, cf. the Data Protection Act[2] § 41, subsection 2, no. 5, cf. subsection 6.

The order must be complied with no later than 5 November 2021. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date.

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 since 2013, complaints have been created in T. Hansen Gruppen A/S' customer system with

three different customer numbers. The telephone number is most often the customer number at T. Hansen Gruppen A/S.

During 2020, the complainant discovered that an unauthorized person's email address and purchases appeared on the complainant's oldest customer profile. The customer number on the profile is the complainant's previous mobile number. The problem was due to the fact that an unauthorized person took over the complainant's previous mobile number, made a purchase at T. Hansen Gruppen A/S, provided the mobile number and the person's e-mail address at the time of purchase, and based on this, the person's purchase and information were added to the complainant's customer profile.

2.1. Complainant's comments

The complainant has generally stated that information about complaints on the complainant's customer profile has been accessed by an unauthorized person, as the person has taken over the complainant's previous mobile number, which T. Hansen Gruppen A/S has used as a customer number. The complainant's customer profile thus contained information about both the complainant and the unauthorized person's name, address, telephone number and purchase from T. Hansen Gruppen A/S.

In addition, complaints have stated that forgotten passwords are stored and sent in clear text at a customer's request. The complainant has tested T. Hansen Gruppen A/S' solution, and the complainant was thus sent his self-selected password in plain text on 25 January 2021 via email. The complainant has stated on this basis that the unauthorized person, who has taken over the complainant's previous mobile number, has been able to have the complainant's password sent to the person concerned's e-mail address.

The complainant has also stated that the unauthorized person's e-mail address in the customer profile at T. Hansen Gruppen A/S has been specified by T. Hansen Gruppen A/S as the profile's primary e-mail address.

2.2. T. Hansen Gruppen A/S' comments

Kromann Reumert has made statements on behalf of T. Hansen Gruppen A/S in the matter.

Kromann Reumert, on behalf of T. Hansen Gruppen A/S, has stated that information about the unauthorized person has appeared in the complainant's customer profile for an unknown period, but presumably from 29 January to 2 February 2021, and at least until at the latest on 9 February 2021.

If the unauthorized person had accessed the complainant's customer profile at T. Hansen Gruppen A/S during this period, the person would have received information about the complainant's name, address, telephone number, e-mail address and

invoice from previous purchases.

If the unauthorized person had clicked on "send password again", this person would have the complainant's password sent in plain text to his e-mail address. The transmission itself would be encrypted on the transport storage with TLS 1.2. In this connection, Kromann Reumert has noticed that the password sent is very likely to be an auto-generated password.

T. Hansen Gruppen A/S has, however, been able to establish that the unauthorized person has neither accessed the web login nor used the "resend password" function.

T. Hansen Gruppen A/S has stated that the company saves or has saved a copy of the complainant's password in plain text or in a form that can be traced back to plain text. By using the "forgot password" function, the complainant could have his password sent in plain text to his provided e-mail address, if the customer number and e-mail on the customer profile matched what the complainant had specified. In that case, the transmission would be encrypted.

T. Hansen Gruppen A/S has – in agreement with the complainant – transferred all the complainant's information, including purchase history, to the complainant's customer profile with the complainant's current telephone number, and deleted one of the complainant's customer profiles and blocked the other customer profile.

Kromann Reumert has stated that the error occurred because the staff at T. Hansen Gruppen A/S had not verified data on the relevant customer profile in connection with the unauthorized person's purchase. The staff should have ensured separation of the two customers' purchase history; either by creating a new customer profile for the unauthorized person, or by having ensured the transfer of the complainant's data to a new customer number.

To prevent similar cases from recurring, T. Hansen Gruppen A/S has on 9 February 2021 closed down the ability of private customers to access web log-in and on 14 April 2021 removed the ability to resend passwords. T. Hansen Gruppen A/S is working on a new log-in solution with a different password policy, where forgotten passwords must be reset instead of being sent via email to the user. Until then, T. Hansen Gruppen A/S has blocked the existing solution. T. Hansen Gruppen A/S has also initiated changes in the company's ERP system, so that data on customer profiles cannot be combined unless a verification of data has been carried out beforehand. This means that all customers who are not completely identifiable will have a new account created with T. Hansen Gruppen A/S when placing an order for goods.

T. Hansen Gruppen A/S has not carried out a risk assessment for sending passwords in clear text via e-mail, but is preparing a risk assessment based on the new web-log solution.

T. Hansen Gruppen A/S has not made a report, as the company has assessed that it is unlikely that the incidents entail a risk to the complainant's rights or freedoms, as there has been no compromise of personal data about the complainant. It has also been assessed that it does not entail a risk to the unauthorized person's rights or freedoms that the complainant has been given access to general information about the person. For the same reason, T. Hansen Gruppen A/S did not inform the person about the incident.

3. Reason for the Data Protection Authority's decision

3.1 Article 32 of the Data Protection Regulation

Based on the information provided in the case, the Danish Data Protection Authority assumes that information about an unauthorized person's name, address, telephone number and purchases from T. Hansen Gruppen A/S was added to the complainant's customer profile at T. Hansen Gruppen A/S, and that the unauthorized person for an unknown period, but presumably from 29 January to 2 February 2021, had access to information about complaints and access to have the complainant's password sent.

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 considers that there has been a breach of personal data security, cf. Article 4, No. 12 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 in 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 diligence of the data controller in ensuring that unauthorized access does not occur to personal data and that all probable error scenarios should be tested in connection with the development of new software where personal data is processed.

Furthermore, the Danish Data Protection Authority is of the opinion that, in connection with processing where users' passwords

are stored in IT solutions that are exposed to networks over which the data controller has no control, it will normally be an appropriate security measure to use a recognized algorithm for encryption (e.g. .e.g. hashing) of passwords, so that these are not stored in clear text at any time.

This applies regardless of which and how much personal data the processing includes. The background for this is that many registered users reuse passwords across services, etc., which is why there is an imminent risk that the password combined with e.g. an email address will be able to provide access to further information on other websites, etc.

On this basis, the Danish Data Protection Authority finds that T. Hansen Gruppen 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 thereby emphasized that T. Hansen Gruppen A/S, when developing its system, did not take into account the risk of customers' information being combined, for example as a result of a telephone number being transferred from one person to another . The Danish Data Protection Authority is of the opinion that the reuse of telephone numbers is a predictable and normally occurring scenario, which is why this should have been included when determining the relevant security measures. The Danish Data Protection Authority has also emphasized that T. Hansen Gruppen A/S has stored the user's self-selected passwords in clear text without a recognized algorithm for irreversible encryption, and that T. Hansen Gruppen A/S has had a function where users have been able to have passwords sent in clear text to the user's specified e-mail address upon request, notwithstanding that T. Hansen Gruppen A/S has not carried out a risk assessment in accordance with this.

The Danish Data Protection Authority also finds grounds to notify T. Hansen Gruppen A/S of an order to - to the extent that T. Hansen Gruppen A/S still stores passwords in plain text - use a recognized algorithm for encryption (e.g. hashing) of all passwords , so that these are not stored or can be restored in plain text.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d. It is noted in this connection that failure to comply with an order from the Data Protection Authority can be punished with a fine, cf. the Data Protection Act § 41, subsection 2, no. 5, cf. subsection 6.

The order must be complied with no later than 5 November 2021. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date.

The Danish Data Protection Authority has noted that T. Hansen Gruppen A/S has shut down private customers' ability to

access web log-in, removed the option to resend passwords and is working on a new log-in solution with a different password policy, where forgotten passwords must be reset instead of being sent via email to the user. The Danish Data Protection Authority has also noted that T. Hansen Gruppen A/S has initiated changes to the company's ERP system, so that data on customer profiles cannot be combined unless a verification of the data has been carried out beforehand.

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 T. Hansen Gruppen A/S - by not reporting the breach to the Danish Data Protection Authority - has not met the requirements of Article 33, paragraph 1 of the Data Protection Regulation. 1.

It is the Danish Data Protection Authority's assessment that the unauthorized access to personal data for complaints about the unauthorized person constitutes a breach of personal data security, which must be reported to the Danish Data Protection Authority. In this connection, the Danish Data Protection Authority has emphasized that all breaches of personal data security must be reported to the Danish Data Protection Authority, unless it is unlikely that the breach of personal data security entails a risk to the rights or freedoms of natural persons. A risk to the rights and freedoms of natural persons includes, among other things, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to confidentiality or any other significant economic or social disadvantage for the data subject. In this connection, the Danish Data Protection Authority is of the opinion that T. Hansen Gruppen A/S has not proved that it is unlikely that the breach of personal data security entails a risk to the rights or freedoms of the unauthorized person.

The Danish Data Protection Authority shall, on this occasion, enforce that T. Hansen Gruppen A/S reports similar security breaches to the Danish Data Protection Authority in accordance with Article 33, paragraph 1 of the Data Protection Regulation. 1.

3.3. Summary

On the basis of the above, the Data Protection Authority finds that there is a basis for expressing criticism that T. Hansen Gruppen A/S' processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1, and Article 33, subsection 1.

The Danish Data Protection Authority also finds grounds to notify T. Hansen Gruppen A/S of an order to - to the extent that T. Hansen Gruppen A/S still stores passwords in plain text - use a recognized algorithm for encryption (e.g. hashing) of all passwords , so that these are not stored or can be restored in plain text.

The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d. It is noted in this connection that failure to comply with an order from the Data Protection Authority can be punished with a fine, cf. the Data Protection Act § 41, subsection 2, no. 5, cf. subsection 6.

The order must be complied with no later than 5 November 2021. The Danish Data Protection Authority must request to receive confirmation that the order has been complied with by the same date.

[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).