Violation of personal data security at nemlig.com A / S

Date: 18-12-2019

Decision

Private companies

The Danish Data Protection Agency issued an order for notification of the data subjects after a breach of personal data security.

Journal number: 2019-441-1578

Summary

The Danish Data Protection Agency has dealt with a total of two related cases of breaches of personal data security (see the decision in the second case here). In both cases, the data controllers had assessed that the data subjects should not be notified. The information was primarily name, contact and address information as well as purchase history.

As there was a significant number of data subjects (more than 250,000) and as the data controllers had not assessed the risk separately for the subset of data subjects who may have a secret or omitted address, the Danish Data Protection Agency made an assessment of the risk for this group of data subjects. . As the Authority assessed the risk for these data subjects to be high, the Danish Data Protection Agency required the data controllers to notify the data subjects who may have a secret or omitted address.

The decision states that even in otherwise homogeneous processing of information, which generally does not have a high risk profile, there may be conditions for the individual data subject that involve a high risk. The risk assessment carried out by the data controller - for whether notification is to be made - must reflect such individual circumstances.

Decision

The Danish Data Protection Agency hereby returns to the case where Nemlig.com A / S (hereinafter "Namely") on 21 January 2019 reported a breach of personal data security to the Danish Data Protection Agency.

Decision

After a review of the case, the Danish Data Protection Agency finds grounds for issuing an order to notify the registered persons, who may have a secret or omitted address. The injunction is granted pursuant to Article 58 (1) of the Data Protection Regulation [1]. 2, letter e.

The content of the notification shall comply with the requirements of Article 34 of the Data Protection Regulation, thus describing in clear language the nature of the breach of personal data security and containing at least the information and measures referred to in Article 33 (2). 3, letters b, c and d.

The deadline for compliance with the order is 7 January 2020. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with, together with an anonymised version of the notification. According to the Data Protection Act, section 41, subsection 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 case that sufficient access control has not been established on a web-based reporting service, so that order information about customers has been available on the Internet. These are approximately. 250,000 customers at Namely. As the notification of the breach of personal data security has been made by Nemlig and taking into account the other information in the case - in particular that Nemlig determines the purpose and means of the processing - Nemlig is considered to be responsible for the data.

Namely, has stated that by going to http://xxx.xxx.xxx.xxx and selecting 'Find Box From Order', and entering a valid order number, there was access to the specific customer's name, address, customer number and the contents of the order in question. The functionality was not available from nemlig.com's main pages.

In response to the Danish Data Protection Agency's inquiry regarding a possible processing of secret addresses, Namely has stated that a delivery address is an absolute necessity for the delivery of goods to customers. Namely, does not register whether an address is secret, as it is irrelevant. Against this background, the risk assessment did not include an assessment of whether secret addresses were included.

Namely, has stated that in order to obtain a valid order, one must have knowledge of what a valid order number looks like, know the number of digits in the number, and know which number series are valid. Without this, no data will emerge. There are no fields or anything from which one can derive information about the format of order numbers. It was possible to try it out until you hit a valid order number.

Furthermore, Namely has stated that at the time of the incident, server logs were available 7 days ago, and these were used to establish that during the period there was no unauthorized access to customer data on the web server.

According to Namely, cleaning up after the breach consisted of a tightening of the firewall rules so that there was no longer access to the web server from the outside.

It appears from Nemlig's notification of the breach that the data subjects concerned will not be notified, and the reasons for this are:

The violation does not involve a high risk to the rights or freedoms of the persons concerned.

Adequate technical and organizational security measures have been implemented to remedy the incident.

Measures taken by the data controller that justify failure to notify the affected persons are: Ensuring that all external access to the service is no longer possible, as well as testing and validation of internal access.

It appears from the case that on 24 January 2019 an assessment was made of whether Namlig is obliged to notify the data subjects pursuant to Article 34 of the Data Protection Regulation.

Fact

Reference is made to the documentation forms for the security breach appendices 3 and 4 (sent to X on 21 January 2019), which are attached to this assessment, and which are the basis for the assessment, including that the internal access to the web-based reporting service has been finally closed at the latest Tuesday, January 22, 2019.

Duty to notify the registered (customers) pursuant to GDPR art. 34?

It follows from GDPR art. 34, that Namlig and Intervare as data controllers in the event of a security breach are obliged to notify the data subjects (customers) if the security breach is likely to entail a high risk for the data subjects '(customers') rights and freedoms. Considering that:

only ordinary personal information (and not sensitive personal information) such as name, address and purchase of goods on the specific order - and only by entering a specific order number, which one must in any case guess at or otherwise obtain - has been available,

Namely, and Intervare have not found that there has been any unusual traffic on the web-based reporting service,

Namely and Intervare has not, via log or in any other way, found that access to the web service has been used unauthorized,

None of the data subjects has notified Namely and / or Intervare that they have experienced that their rights or freedoms have

not been violated during the period in which the unauthorized access has been possible,

There is no indication that the security breach has had consequences for the data subjects,

As a consequence of the above, it is not probable that the unauthorized access has been used and that there has not been a high risk to customers' rights and freedoms, and

Namely and Intervare immediately after finding the security breach has taken the necessary organizational and technical measures (which are closed to external access on the firewall and access control has been established on the individual report service), cf. GDPR art. 34, 3 (b),

it is our assessment that Namely and Intervare is not obliged to notify the data subjects pursuant to GDPR art. 34, 1.

Justification for the Danish Data Protection Agency's decision

As a result of the notification from Namlig, the Danish Data Protection Agency assumes that there has been a breach of personal data security.

The Danish Data Protection Agency does not consider that an assessment has been carried out in accordance with Article 34 (1) of the Data Protection Regulation. 1, of the risk to the data subjects' rights. The Danish Data Protection Agency has emphasized the following in particular.

It does not appear that Namely has assessed the risk that the individual addresses could be secret / protected. In the opinion of the Danish Data Protection Agency, secret / protected addresses constitute confidential personal information, and an unintentional exposure of such information can potentially have serious consequences for the data subjects' rights. Given the high number of data subjects, it is the Data Inspectorate's view that the security breach has most likely affected someone where exposure of their address could have a high consequence, and thus the Data Inspectorate's view is that the breach poses a high risk to these data subjects.

Namely, the risk assessment emphasizes that no unusual traffic or unauthorized use of the access has been found. In this connection, reference is made to a log. The Danish Data Protection Agency understands the circumstances in such a way that the log only shows applications of the access in the last 7 days. The Danish Data Protection Agency does not find that a 7-day log - in addition to one week - can in any way substantiate whether unauthorized access has been made to the information, which has been available via the Internet from 2016 to January 2019.

The Danish Data Protection Agency does not find that the format of the Internet address (URL) is so unique that this in itself

provides any protection against unauthorized use. Furthermore, the Authority does not find that lack of knowledge of the format of a valid order number provides any protection, as it was possible to try out without restrictions on the number of attempts. Furthermore, several orders per. customer and over a quarter of a million customers (Namely and Interware's customers combined) entail many opportunities to hit right on the guess of a ten-digit order number.

The Internet address (URL) that could be used from the Internet (http://xxx.xxx.xxx.xxx) does not in itself indicate whether the transmission of the personal data took place with or without the use of encryption. The Danish Data Protection Agency finds that such an aspect should have been included in the risk assessment when the breach includes the possible transmission of confidential personal data over the Internet - including the employees' authorized use of the web-based reporting service.

Nemlig's risk assessment emphasizes that none of the data subjects have notified Nemlig and / or Intervare that they have experienced that their rights or freedoms have not been violated during the period in which the unauthorized access has been possible. The Danish Data Protection Agency assumes that this is a clerical error, and it is believed that none of the data subjects have stated that their rights have been violated during the period in which the violation took place.

Namely, however, can not expect that a data subject who experiences misuse of information about a secret address will necessarily be able to link this to specifically Namlig's processing of the address. The address may be registered with several private companies and public authorities. Furthermore, the customer may not necessarily remember that Namely is in possession of the address, e.g. if the customer has not shopped at Namely since 2016. Finally, information about addresses may have been retrieved by unauthorized persons for the purpose of misuse at a much later date.

Namely, has stated that the data subjects will not be notified and this is justified by measures concerning the closure of the unauthorized access. This is repeated in the risk assessment, where reference is also made to Article 34 (1) of the Data Protection Regulation. 3, letter b.

In this connection, the Danish Data Protection Agency should note that Article 34, para. 3, points to the data subjects, as referred to in para. 1, and it deals with the data subjects for whom the breach involves a risk. The primary purpose of notifying individuals of security breaches is to provide them with specific information on what precautions they should take to protect themselves from potential consequences of the breach. [2]

The risk assessment must concern the data subjects who are affected by the breach. The described measures implemented by Namely only work in the future, and will therefore not change the risk that the breach has already posed for a number of

years, and may still pose to the data subjects who are affected by the breach. If some of the registered personal data has come to the knowledge of unauthorized persons, the risk thus remains unchanged from the measures described, and the measures do not mean that the high risk to the data subjects' rights and freedoms is probably no longer real.

The Danish Data Protection Agency does not find that Namely can refrain from notifying the data subjects with reference to Article 34 (1). 3, letter b, as the conditions are not seen to be met.

On the basis of the above, the Danish Data Protection Agency finds that Namely must have carried out a new assessment of the risks that the breach of personal data security poses to the data subjects' rights and freedoms.

As it has not already notified the data subjects of the breach of personal data security, the Danish Data Protection Agency has, based on the circumstances described in the case, considered the likelihood that the breach of personal data security entails a high risk, cf. On that basis, the Authority has chosen to issue an order to the data controller nemlig.com A / S, cf. Article 58 (1). 2, letter e, to inform the data subjects concerned, who may have a secret or omitted address. If data subjects with a secret / omitted address cannot be identified, all affected data subjects will be notified (approx. 250,000).

The notification shall comply with the requirements of Article 34 of the Data Protection Regulation, thus describing in clear language the nature of the breach of personal data security and containing at least the information and measures referred to in Article 33 (2). 3, letters b, c and d. This means, among other things, that if confidential personal information may have been transmitted over the Internet without the use of encryption, this must be included as part of the description of the nature of the breach.

[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] See Recital 86 of the Data Protection Regulation and the Article 29 Working Party "Guidelines on Notification of Personal Data Security Violations under Regulation 2016/679" (WP250 rev.01).