Unencrypted email with personal information sent from the Ministry of Justice

Date: 19-05-2021

Decision

Public authorities

The Danish Data Protection Agency has investigated a breach of personal data security in the Ministry of Justice's department. The Authority found that the Ministry of Justice had not proved that the information had been processed with the necessary security. The Authority expresses serious criticism and has ordered the Ministry of Justice to inform the data subjects.

Journal number: 2020-442-6885

Summary

The Ministry of Justice sent an e-mail to the Danish Bar Association with information about 35 people's name, social security number and, among other things. reminder letters regarding. submission for recovery of fines in SKAT.

The e-mail was sent outside the normally encrypted channels, and it could not be documented whether the e-mail had been sent encrypted.

The Danish Data Protection Agency expressed serious criticism of the Ministry of Justice for having acted in violation of the rules of the Data Protection Regulation, both in sending the e-mail and in handling the breach.

Particularly problematic was the fact that approx. three months, from the time the ministry was informed of the potential breach until it was investigated. This led to a delayed notification to the Danish Data Protection Agency. This probably also contributed to the fact that it could not be clarified with certainty how the e-mail had been transmitted over the Internet.

One of the criticisms concerns the fact that the Ministry of Justice, after three months of investigating the breach, has not yet decided whether the data subjects concerned should be notified of the breach. The Ministry later stated that it had decided not to notify, but without this being based on new information in the case, the Danish Data Protection Agency therefore found that the decision should have been made earlier.

The Danish Data Protection Agency also disregarded the Ministry of Justice's assessment that notification should not take place. The Danish Data Protection Agency found that the risk assessment had not addressed the potential loss of rights of the specific data subjects, but only had a general focus on the fact that the Ministry had no knowledge of realized consequences. Primarily, the focus was on the fact that the ministry had not been informed that unauthorized persons had accessed the

e-mails, the possibility of e.g. loss of reputation or future business was not part of the assessment.

The Authority is of the opinion that a data controller will often not be the first to hear about a possible misuse, and in cases where the consequences of unlawful access may lie in the future, concrete lack of knowledge about realized consequences is not necessarily something that can greater importance is attached to the assessment of what risks a breach poses to the data subjects.

When the Danish Data Protection Agency assessed the risk as high, the Ministry of Justice was required to notify the data subjects of the breach.

Decision

The Danish Data Protection Agency hereby returns to the case where the Ministry of Justice's (hereinafter the Ministry of Justice) on 28 February 2020 reported a breach of personal data security to the Danish Data Protection Agency. The review has the following reference number:

5ab99649e03f313dd9e6f56a4138394631bede54.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Ministry of Justice's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. 1 cf. Article 24, 33, para. 1 and 34, para. 1.

At the same time, the Danish Data Protection Agency finds that there are grounds for issuing an order to the Ministry of Justice to notify all data subjects who are affected by the breach. The order is issued 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 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 deadline for compliance with the order is 1 June 2021. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with and an anonymised version of the notification.

According to the Data Protection Act [1] § 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

On 28 February 2020, the Ministry of Justice reported a breach of personal data security to the Danish Data Protection Agency.

The notification states that the Ministry of Justice has sent an e-mail with personal information about 35 people, and that this shipment presumably took place over the Internet without the use of encryption.

3. Comments of the Ministry of Justice

It appears from the case that on March 27, 2019, an email was sent from the Department of Justice to the Bar Association. This email contained information about 35 people. The information includes name, social security number and financial circumstances in the form of invoices and reminder letters regarding. submission for recovery of fines in SKAT.

On 18 November 2019, the Ministry of Justice receives an inquiry from a lawyer raising doubts as to whether the email sent on 27 March 2019 was sent with or without the use of encryption. The employee who had sent the e-mail was no longer employed and the sent e-mail was no longer accessible. The Ministry of Justice launched an internal investigation that did not clarify the matter, and later also an investigation with the Ministry of Justice's operations supplier, Statens It.

On 3 February 2020, Statens It states that they have received the assignment and will return before 7 February 2020.

On 26 February 2020, the Ministry of Justice received a reply from Statens It, stating that it cannot be clarified whether the e-mail in question was sent with or without the use of encryption, but that it must be assumed that the shipment took place without the use of encryption. It also appears that part of the challenge in clarifying this is the time that has elapsed since the email was sent. The Ministry of Justice concluded on the same day, 26 February 2020, that the relevant e-mail had probably not been sent encrypted, and there was therefore a breach of personal data security.

On 28 February 2020, the Ministry of Justice will report the incident as a breach of personal data security.

On 24 April 2020, the Danish Data Protection Agency will send a hearing to the Ministry of Justice with a response deadline of 15 May 2020. The Ministry of Justice will retain the hearing on 2 July 2020.

In the investigation of the e-mail sending, Statens It has stated, among other things, that:

"We do not have logs that long back…"

“It can hardly have been sent securely from KRFO´'s system, as the recipient p.t. does not have its own certificate and the company does not support tunnel mail. ”

The Ministry of Justice's documentation of the circumstances of the breach consists of the notification to the Danish Data Protection Agency. In addition, the Ministry of Justice has responded to the Authority's hearing. These documents highlight, among other things, the following regarding the circumstances of the breach:

“Unencrypted transmission of personal information entails a risk that unauthorized persons may gain access to the information in question. However, there are no indications that unauthorized persons have had access to the information concerned in the specific case. "

"However, there are no indications that the incident has had consequences for those registered in the case."

"There are no indications that unauthorized persons have become aware of the information concerned or that the data subjects have suffered damage."

At the time of reporting the breach to the Danish Data Protection Agency, on 28 February 2020, the Ministry of Justice had not yet decided whether to notify the data subjects concerned. In a reply of 2 July 2020 to the supervision hearing, the Ministry of Justice states that the data subjects will not be notified on the following grounds:

"The Ministry of Justice can state that the Ministry has assessed that the data subjects must not be notified in accordance with Article 34 of the Data Protection Regulation.

In this connection, the Ministry of Justice has emphasized that this was an email sent from the Ministry of Justice to the Danish Bar Association, where there has probably been no encryption in connection with the transmission of the e-mail.

Thus, there is no personal data that has been lost or that has been published. It is also the Ministry's assessment that the personal data in connection with the transfer to the Danish Bar Association has only potentially been available to unauthorized persons for a relatively short period. At the same time, there are no known indications from the Ministry of Justice that unauthorized persons have actually gained access to the information.

In relation to the consequences of the security breach for the data subjects, it must therefore be emphasized that it is not certain that the unencrypted e-mail has come to the knowledge of unauthorized persons during the short period in which the information has been available. ”

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

On the basis of what the Ministry of Justice has stated, the Danish Data Protection Agency assumes that an e-mail has probably been sent via the Internet with personal data worthy of protection, without encryption being used. It is further assumed that the Ministry of Justice has not been able to prove whether encryption has been used or not.

On this basis, the Danish Data Protection Agency assumes that there has been a potentially illegal access to personal data, which is why the Authority finds that there has been a breach of personal data security, cf. Article 4, no. 12 of the Data Protection Regulation.

The Danish Data Protection Agency also assumes that the 35 data subjects concerned were lawyers and that the information on debt concerned the activities of these lawyers.

4.1. Article 32 of the Data Protection Regulation

It follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks involved in the data controller's processing of personal data.

Thus, the data controller 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 put in place to protect the data subjects against these risks.

In addition, according to Article 24 of the Data Protection Regulation, the data controller has a duty to be able to demonstrate that processing takes place in accordance with the Regulation.

The Danish Data Protection Agency is of the opinion that the requirement pursuant to Article 32 for appropriate security will normally mean that it will be an appropriate security measure to use encryption when transmitting confidential and sensitive personal data by e-mail via the Internet and that the handling of many persons' personal data in one and the same shipment places greater demands on the employees' diligence in connection with shipment.

Against this background, the Danish Data Protection Agency finds that the Ministry of Justice - by having provided information on 35 persons' names, social security numbers and debt information without being able to document the use of encryption - has not taken appropriate organizational and technical measures to ensure an appropriate level of security. the risks involved in the processing of personal data by the Authority in accordance with Article 32 (2) of the Data Protection Regulation; 1 in accordance with Article 24.

4.2. Article 33 of the Data Protection Regulation

It follows from Article 33 (1) of the Regulation 1, that the data controller in the event of a breach of personal data security without undue delay and if possible within 72 hours must report the breach to the Danish Data Protection Agency, unless it is unlikely that the breach of personal data security entails a risk to natural persons' rights or freedoms.

The Danish Data Protection Agency therefore finds that the Ministry of Justice's processing of personal data - in that the Ministry of Justice did not ensure faster clarification and contact with Statens IT and thus faster and timely notification to the Danish Data Protection Agency - has not taken place in accordance with Article 33 (1). 1.

In this connection, the Danish Data Protection Agency has emphasized that the Ministry of Justice was informed of a possible breach on 18 November 2019, but only reported a breach to the Danish Data Protection Agency on 28 February 2020. In the meantime, the Ministry of Justice conducted its own investigation. first became involved in the investigation, much later, from 3 February 2020.

In such investigations, it can make a difference how quickly one responds, in that logs disappear over time, and an early contact with an IT supplier can thus provide more and more accurate answers. Statens IT also seems to state that logs are not stored for so long that they could be used for the investigation. However, the Danish Data Protection Agency is of the opinion that it is not certain that these logs would have been useful for the investigation, even if the Ministry of Justice had approached Statens IT already on 18 November 2019, but nevertheless the Ministry of Justice should have clarified this much earlier in the course.

It is therefore the Authority's opinion that the more than 3 months that elapsed before the notification to the Danish Data Protection Agency are an unnecessary delay, as the factual information could and should have been clarified earlier.

In this connection, the Danish Data Protection Agency must refer to the fact that the provision provides for the possibility of making a preliminary notification, which can then be elaborated, corrected or corrected, with further facts at a later date.

4.3. Article 34 of the Data Protection Regulation

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

The Danish Data Protection Agency finds that the Ministry of Justice's processing of personal data - by not notifying the data subjects of the breach of personal data security - has not taken place in accordance with Article 34 (1) of the Data Protection

Regulation. 1.

Assessment of risks for the data subjects

The Ministry of Justice's documentation of the circumstances of the breach emphasizes several times that there are no indications that unauthorized persons have become aware of the information in question. The Ministry of Justice has not stated in its documentation why this is given special importance.

The reasoning for not informing the data subjects is emphasized somewhat similarly, in that the argument includes the fact that the Ministry of Justice is not aware of any indications that unauthorized persons have in fact been given access to the information.

In this connection, the Danish Data Protection Agency must note that the transmission of data over the Internet without the use of encryption is a type of "hidden" access to the information over which the data controller has no control. This may involve the processing of data by unauthorized actors who are neither data processors nor IT suppliers for the Ministry of Justice, and any misuse of data can therefore not be expected to come to the attention of the Ministry of Justice.

The Danish Data Protection Agency therefore does not find that in the vast majority of situations it can be expected that the data controller will be informed if someone intercepts the e-mail during its transmission over the Internet. The fact that the Ministry of Justice is not aware of access to data therefore does not change the risk that the breach poses to the data subjects, except that a knowledge of interception would have realized the risk in question as having occurred. Therefore, this type of consideration of lack of knowledge of unauthorized access - in general - should not be included in a risk assessment under Article 34 (1). 1, which concerns the notification of the data subjects. Nor is it a matter that should be included in a notification of the data subjects, as it may give the data subject a misleading impression of the risk.

The Danish Data Protection Agency must also note that it is precisely the potential access to the information in clear text that is the core problem, as unauthorized persons will always be able to access information contained in an e-mail transmission when this is done over the Internet without the use of encryption. The risk (possibility of danger) for the data subjects primarily concerns whether someone chooses to use an acquired access to misuse the information.

Assessment of consequences for the data subjects

In relation to the consequences for the data subjects, the Ministry of Justice emphasizes that there are no indications that the incident has had consequences for the data subjects. It is linked to the information that it is not certain that the e-mail has

come to the knowledge of unauthorized persons.

In this connection, the Danish Data Protection Agency must note that an assessment of the consequence for the data subjects is an important element in the assessment of risks in the event of the breach, and thus also whether the risk for the data subjects is high, after which notification must be given.

The Ministry of Justice's assessment of consequence seems to primarily or exclusively concern the lack of knowledge about consequences and the lack of knowledge about whether the e-mail has come to the knowledge of unauthorized persons. The Ministry of Justice is not seen to have assessed what potential consequences it may have or would have had if the e-mail had been accessed by unauthorized persons and the personal data had been misused. The e-mail contained, among other things, information on financial matters and information on recovery, etc., which in the Data Inspectorate's opinion may have significant consequences for the person's business opportunities as a lawyer, and which could have a negative effect on their business. The Department of Justice is not seen to have included this or the possibility of identity theft, phishing attacks or other commonly occurring threats, in its assessment of potential consequences of the breach.

Misuse of social security number and name can e.g. used in attempted identity theft. However, as the name and social security number are processed in many contexts, and since the data subjects concerned were not notified of the breach, the data subjects have no reason to link an identity theft to this particular e-mail transmission, and they can therefore not be expected to contact and inform the Ministry of Justice. herom.

Furthermore, a misuse of personal data can occur long after the breach has occurred, and the consequences can thus be future. This is another reason why, in this case, the lack of current knowledge about realized consequences can not be given any greater significance in its assessment of risks.

It is the opinion of the Danish Data Protection Agency that the Ministry of Justice can not be said to have made a real assessment of the risks that the breach has posed and can still pose to the data subjects' rights, which is critical for a correct assessment of whether the data subjects should be notified of the breach. Article 34 (1) 1.

The Authority's assessment of risks

The Danish Data Protection Agency understands the case in such a way that the e-mail was in all probability sent without the use of encryption, as the Ministry of Justice's IT suppliers have made a thorough investigation which shows, among other things, that the recipient of the e-mail did not have his own certificate. mail. The Danish Data Protection Agency thus

understands that the IT supplier does not believe that at the time of sending the e-mail there was a technical possibility to use encryption of the e-mail's content or encryption of the transmission channel.

It is the Data Inspectorate's opinion that breaches of personal data security regarding information worthy of protection, including information on social security numbers, debt conditions, recovery, etc. in the context of a law firm, which in principle entails a high risk for the rights of the data subjects concerned, as exposure to such information may involve serious violations of these, both violations of integrity and damage to reputation.

The Danish Data Protection Agency is of the opinion that in cases such as the present, notification must be made in accordance with Article 34 of the Data Protection Regulation, as the breach is likely to involve a high risk to data subjects' rights and freedoms, for example in the form of identity theft, breaches of integrity or damage to their reputation. lawyers.

In this connection, the Danish Data Protection Agency has emphasized that the Ministry of Justice is not seen as having documented and substantiated circumstances that indicate that the violation does not involve a high risk to the rights and freedoms of natural persons, which could justify not notifying the registered on the breach of personal data security.

The Danish Data Protection Agency has further emphasized that when there are several affected data subjects, the probability increases that for at least one of these has a high consequence if the exposed personal data is misused. It also increases the chances of abuse when there are several names and social security numbers to choose from for e.g. to attempt identity theft.

Delay in the Ministry of Justice's assessment

Finally, it should be noted that the Ministry of Justice's argumentation in the consultation response to the Danish Data Protection Agency on 2 July 2020, regarding failure to notify, is not seen as containing anything new in relation to what the Ministry of Justice already knew at the time of reporting the breach. Furthermore, given that the notification took place more than three months after the Ministry of Justice was informed of the potential breach, and that the conclusion that a breach had taken place was made on 26 February 2020, there is no reason why notification of the data subjects has not yet been was decided at the notification to the Authority on 28 February 2020.

Delay in taking notice may in itself have a negative effect on the data subjects concerned, who in a period of ignorance of the breach cannot take precautions to protect themselves.

4.4. Summary

On the basis of the above, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that

the Ministry of Justice's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. 1 cf. Article 24, 33, para. 1 and 34, para. 1.

The Danish Data Protection Agency has hereby emphasized the following as aggravating circumstances:

That there are 35 registered.

That the breach has affected personal data worthy of protection.

That notification of the data subjects concerned has been omitted on an incorrect basis.

That the handling of the breach has taken place in a way that has delayed the notification to the Danish Data Protection Agency and the notification of the data subjects.

The Danish Data Protection Agency also finds grounds for issuing an injunction from the Ministry of Justice pursuant to Article 58 (1) of the Data Protection Regulation [2]. 2, letter e, to notify all data subjects of the breach of personal data security.

[1] 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).

[2] 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).