Sensitive information in unencrypted mail from Silkeborg Municipality

Date: 25-11-2021

Decision

Public authorities

Serious criticism

Reported breach of personal data security

Sensitive information

Unsafe transmission

Treatment safety

The Danish Data Protection Authority has expressed serious criticism that Silkeborg Municipality did not have adequate security measures when the municipality sent confidential and sensitive information in an unencrypted e-mail.

Journal number: 2021-442-11601.

On 3 February 2021, Silkeborg Municipality reported a breach of personal data security. The review has reference number: 9e8f54e07f09548bd3da0b89ac216bcb3d34b593.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that Silkeborg Municipality'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 5, subsection 2, cf. Article 5, subsection 1, letter f.

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 notification that Silkeborg Municipality sent an e-mail to Denmark's Statistics Consulting on 3 February 2021. The e-mail contained a list with social security number, school name and school code for 12,915 school pupils. It appears from the report that the e-mail was not sent securely and thus not encrypted from sender to recipient.

3. Reviewer's comments

Silkeborg Municipality has stated in the notification of 3 February 2021 and the subsequent consultation response of 5 July 2021 that the municipality sent an e-mail to Denmark's Statistics Consulting on 3 February 2021. The e-mail contained a list with social security number, school name and school code for 12,915 school pupils. The email was not sent securely. It also appears that it was a matter of human error, as an employee – who was aware of the guidelines for sending e-mails securely – happened to send the e-mail insecurely by pressing the wrong button.

On 12 August 2021, at the request of the Danish Data Protection Authority, Silkeborg Municipality stated that TLS 1.1 encryption was implemented in the municipality at the time the e-mail was sent, which is why the e-mail in question could possibly be encrypted at the transport layer with TLS 1.1.

The municipality contacted the recipient soon after sending and ensured that the e-mail had reached the correct recipient.

Silkeborg Municipality has – in order to strengthen all employees' level of knowledge and attention to, among other things, the use of correct e-mail sending – prepared a video course for all employees regarding GDPR, just as the correct use of shipping methods is continuously being strengthened in relevant contexts.

Furthermore, from August 2021 the municipality will introduce TLS 1.2 encryption on all e-mail shipments, which is why it is the municipality's opinion that repeat cases will not be possible, as e-mails will always be sent via an encrypted connection.

4. Reason for the Data Protection Authority's decision

On the basis of Silkeborg Municipality's information, the Danish Data Protection Authority assumes that the municipality has not been able to document that the transmission took place using encryption, neither on the transport layer nor in the content of the e-mail.

The Norwegian Data Protection Authority further assumes that if the email in question was encrypted, it was only on the transport layer and with TLS 1.1.

Article 32, subsection of the Data Protection Regulation. 1, states that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing in question as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, implements appropriate technical and organizational measures in order to ensure a level of security appropriate to these risks.

The Danish Data Protection Authority is of the opinion that encryption on the transport layer with a sufficiently strong algorithm and key should normally be considered a minimum level of security when sending confidential and/or sensitive personal data via e-mail. In addition, the authority is of the opinion that there will be types of processing where encryption of the payload, so-called end-to-end encryption, will be appropriate if there is concretely a higher risk with the processing. This could, for example, be the situation if a data controller – as in this case – has to send personal data of a confidential and/or sensitive nature about a large number of data subjects, or the sending of a plurality of confidential and/or sensitive information takes place on a fixed basis.

It is therefore the Danish Data Protection Authority's opinion that encryption on the transport layer using TLS is not sufficient security in all cases when a lot of confidential and/or sensitive personal data is sent. Furthermore, it is the opinion of the authority that TLS 1.1 – which was implemented in Silkeborg Municipality at the time – based on known security weaknesses cannot be considered as adequate security for encryption at the transport layer.

It appears from the case that Silkeborg Municipality had internal guidelines, which stated that e-mails containing citizens' personal data had to be sent securely and encrypted and that the employee in question knew about these guidelines. It also appears from the case that the employee – despite this knowledge – sent the e-mail with a very large amount of confidential personal data relating to children, without making sure that the e-mail was sent securely and encrypted.

It is the Danish Data Protection Authority's assessment that a municipality that processes large amounts of confidential and/or sensitive personal data about citizens must ensure that large data sets are sent in a way where the information is readable also by a third party who receives the e-mail by mistake, why the municipality must have routines that ensure that the content of this type of shipment is also encrypted, and not only encrypted at the transport layer with TLS. This obligation applies in particular when large amounts of confidential and/or sensitive personal data are processed and when the personal data relates to children who enjoy special protection in the data protection regulation.

By not ensuring that the personal data in question was sent with encryption of the content, Silkeborg Municipality has violated the data protection regulation, article 32, subsection 1.

In addition, the Danish Data Protection Authority finds that the use of TLS version 1.1 for encryption at the transport layer cannot be considered to be adequate security for encryption at the transport layer.

In the specific case, Silkeborg Municipality has not been able to explain whether the e-mail was encrypted at all or not, which is why the Danish Data Protection Authority finds that the municipality has violated the data protection regulation's article 5, subsection 2, cf. Article 5, subsection 1 liter f.

The Danish Data Protection Authority emphasizes that it is essential that the data controller's documentation reflects the risks the processing has for the rights of the data subjects and that for a specific processing there is documentation that the chosen security has actually been observed.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Silkeborg Municipality'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 5, subsection 2, cf. Article 5, subsection 1, letter f.

[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).