Supervision of processing security at office community of law firms

Date: 05-11-2019

Decision

Private companies

Journal number: 2019-41-0029

Summary

In 2019, the Danish Data Protection Agency carried out a planned inspection of an office community of law firms. The Authority focused on processing security, including in particular the encryption of e-mails, in accordance with Article 32 of the Data Protection Regulation.

In connection with the supervision, the Danish Data Protection Agency has expressed criticism that the office community has not complied with the requirements of Article 32 (1) of the Data Protection Regulation. 1, and artikel 5, stk. 2, cf. Article 32 (1) (f) 1 and 2.

The Danish Data Protection Agency's concluding statement states, among other things, that the office community had not introduced procedures prior to the inspection visit that ensure that encryption is used on the transport layer via TLS to send confidential and sensitive personal information to clients, etc. over the Internet. Following the inspection visit and before the Data Inspectorate's opinion, the office community has stated that the office community has now introduced procedures that, in case of doubt, ensure that the recipient domain's support for TLS is examined prior to sending an e-mail containing confidential or sensitive personal information.

In addition, the opinion states that the office community has not demonstrated that it has prepared a risk assessment that takes a position on the risk associated with the transmission of confidential and sensitive personal data over the Internet, prior to the inspection visit.

You can read the Danish Data Protection Agency's guiding text on encrypting e-mails here.

Decision

An office community consisting of law firms was among the companies that the Danish Data Protection Agency had selected for supervision in the spring of 2019.

The Data Protection Authority's planned supervision focused on processing security, including in particular the encryption of

e-mails, in accordance with Article 32 of the Data Protection Regulation.

At the request of the Danish Data Protection Agency, in the spring of 2019, in connection with the inspection visit, the office community filled in a questionnaire and submitted this as well as additional material to the inspection. The inspection visit took place on 21 March 2019.

Following the audit of the office community, the Danish Data Protection Agency finds reason to conclude in summary:

That the office community - in accordance with Article 32 of the Data Protection Regulation - uses end-to-end encryption when exchanging S / MIME certificate over the tunnel mail community (hereinafter referred to as tunnel mail) for the transmission of confidential and sensitive personal information over the Internet to police, courts and other recipients the public tunnel list.

That the office community had not prior to the inspection visit introduced procedures that ensure that encryption is used on the transport layer via TLS for the transmission of confidential and sensitive personal information to clients, etc. over the Internet.

That the office community does not - in accordance with Article 5 (1) of the Data Protection Regulation 2, cf. Article 32 (1) (f) 1 and 2 - have demonstrated that they have prepared a risk assessment that addresses the risk associated with the transmission of confidential and sensitive personal data over the Internet, prior to the inspection visit.

That the office community is not aware of any cases where confidential or sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.

Overall, the Danish Data Protection Agency finds reason to criticize the fact that the office community has not complied with the requirements of the Data Protection Regulation in relation to points 2 and 3.

A more detailed review of the Danish Data Protection Agency's conclusions follows below.

Use of encryption when transmitting confidential and sensitive personal information over the Internet

During the inspection visit, the office community confirmed that the covered law firms use the same technical solution for sending encrypted e-mail.

Furthermore, prior to the inspection visit, the office community has stated that the office community sends confidential and sensitive personal information via e-mail over the Internet. Following the inspection visit, the office community has clarified that it is only extremely rare for the office community to send sensitive personal information via e-mail.

2. About the encryption solution

The office community has stated that all e-mail traffic is sent over a TLS 1.2 connection to the data processor's server, from

where the actual encryption is performed. Here are three possible solutions that are used in order of priority:

Send the secure solution, which uses S / MIME with Nets OCES certificates to send end-to-end encrypted to the recipient.

Tunnel mail, which also uses S / MIME with Nets OCES certificates to send encrypted between main mailboxes, but which supports sending from / delivery to the end users' own mailboxes at both ends. The data processor has stated that the tunnel mail solution is supported by over 1,500 recipient domains.

Delivery of e-mail with encryption on the transport layer via opportunistic TLS, if a Nets OCES certificate can not be found for the recipient's e-mail address.

With S / MIME encryption, Nets' database of OCES certificates is automatically searched. The S / MIME encryption uses the AES-256 algorithm, and all private and public keys have a length of 2048 bits.

The office community has also stated that the Send Secure solution and tunnel mail (points 1 and 2 above) for the sender are integrated in Outlook with another button for sending e-mail with the text "Send Secure". By pressing this button, an examination is made of whether the specified recipient address can receive encrypted e-mail either via the Send secure solution or via the tunnel e-mail solution. If the receiver supports one of the two mentioned solutions, the field will be marked in green and otherwise in red. If the recipient does not support one of the solutions, the sender can choose to send the email anyway. In that case, the sending takes place with opportunistic TLS without any guarantee that the e-mail will be sent encrypted.

3. E-mails to the courts, police districts, the prosecution, agencies and boards

Prior to the inspection visit, the law firm has stated that law firms send emails containing confidential or sensitive personal information to the courts, police districts, the prosecution, agencies and boards. These emails are sent either to a main mailbox or directly to an employee's email address.

The office community has stated that when sending such emails, either the Send Secure solution or the Tunnel Mail solution (points 1 and 2 under section 2) is used, which uses S / MIME certificates to perform end-to-end encryption.

The office community has stated that the e-mails in question are sent in professional contexts where the office community represents a client. This may, for example, involve communication with the courts in a specific criminal case, etc., cases concerning the search of a telephone, agreements with the police on interrogations, and when the office community complains to the Danish Prison and Probation Service on behalf of clients, etc.

3.1. Summary

Based on the information provided by the office community, the Danish Data Protection Agency assumes that the office community uses end-to-end encryption with S / MIME certificates to the extent that confidential and sensitive personal information is sent over the Internet to professional actors, including the police, courts and other recipients. on the public tunnel list. The Danish Data Protection Agency thus finds that the office community applies sufficient processing security when sending such e-mails.

4. E-mails to clients etc.

The office community has stated that the office community communicates in different ways with clients, all depending on the individual client.

In relation to detainees, the office community has stated that the office community does not communicate with this group of clients via e-mail, and that communication with these typically takes place by telephone.

In relation to homeless clients and other clients who are exempt from using e-mail or who do not use e-mail as a form of communication, the office community has stated that communication with this group of clients takes place by telephone or in person.

In relation to clients on a free footing, the office community has stated that communication with them takes place via e-mail, SMS, physical letter, telephone and physical attendance.

During the audit visit, the office community stated that when sending emails to clients that do not support the end-to-end encryption solution used by the office community, opportunistic TLS is used in the transmission.

4.1. Cases where encryption has not been used

Prior to the inspection visit, the office community stated that it had occurred that after 1 January 2019, the office community had erroneously sent e-mails with sensitive and confidential information unencrypted over the Internet.

During the inspection visit, the Danish Data Protection Agency asked how often since 1 January 2019 it had happened that the law firms had erroneously sent e-mails with confidential or sensitive information unencrypted over the Internet.

In addition, the owner of one of the law firms stated that the person in question approx. once a week since 1 January 2019 has answered an e-mail from a client - typically using the answer button so that the original inquiry appears below the answer. At the same time, the person in question stated that the person in question was not aware of how many of the inquiries had

contained confidential or sensitive information, but that this had probably been the case for some of them.

The proprietor of one of the other law firms stated that this had been the case less than 10 times, and the proprietor of the last law firm stated that it had happened a maximum of a handful of times.

Asked during the inspection visit, the law firms stated that the recipient of the e-mails in question was the client or a relative of the client, and that the e-mails in question contained information about the client.

However, following the audit visit, the office community has stated that it is not correct that emails have been sent unencrypted over the Internet with confidential or sensitive personal information. The office community has stated that the e-mails in question were sent securely via an opportunistic TLS connection, and that the e-mails in question only contained confidential personal data in quite a few cases and that they did not contain information of a sensitive nature. The office community has subsequently sent a list of the 16 recipient domains to which the e-mails in question have been sent, all of which are seen to support TLS.

4.2. Summary

Based on the information provided by the office community, the Danish Data Protection Agency assumes that the office community uses opportunistic TLS to the extent that the office community sends e-mails over the Internet to clients and relatives, etc., where these recipients do not support the office community's end-to-end solution. encryption.

On the basis of the list of recipient domains submitted by the office community, the Danish Data Protection Agency assumes that the office community is not aware of cases where confidential and sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.

5. Risk assessment

Prior to the audit visit, the office community had submitted a risk assessment for the processing of personal data. However, the submitted risk assessment did not contain considerations in relation to the sending of e-mails containing personal data. The office community stated during the inspection visit in this connection that no such risk assessment had been prepared.

Following the inspection visit, the office community has informed the Danish Data Protection Agency that new procedures have been introduced for the use of opportunistic TLS for sending to clients, etc. Under the new procedures, the sender will - based on an assessment of the recipient's email domain and the content of the email - assess whether the email can be sent with opportunistic TLS. The office community has also stated that in case of doubt, either an inquiry is made into the recipient

domain's support for TLS, or that a blank e-mail is sent with a request for a receipt, after which the receipt e-mail header is examined for use of TLS.

Following the audit, the office community has also confirmed that no written risk assessment had been prepared and stated that the office community's procedures for the specific assessment of e-mail contact with the office community's clients, cf. the section above, have now been incorporated into the office community's existing risk assessment.

5.1. Summary

It is the Data Inspectorate's assessment that the office community has violated Article 5 (1) of the Data Protection Regulation. 2, cf. Article 32 (1) (f) 1 and 2 by not being able to present a written risk assessment during the inspection visit, which identifies the risks that the processing in question poses to the data subjects' rights, as well as an assessment of which technical and organizational measures are appropriate to ensure an appropriate level of security. to these risks, or could otherwise demonstrate that such a risk assessment had been made.

The Danish Data Protection Agency assumes that the office community has not been aware prior to the inspection visit whether the recipient domain supports TLS when e-mails containing confidential or sensitive personal information have been sent to clients, etc.

Furthermore, the Danish Data Protection Agency assumes that the office community has, after the inspection visit, introduced procedures that, in case of doubt, ensure that the recipient domain's support for TLS is examined prior to sending an e-mail containing confidential or sensitive personal information.

It is the Danish Data Protection Agency's assessment that the office community's lack of risk assessment in relation to the transmission of e-mails containing personal data has led to insufficient security measures in relation to e-mails to clients and relatives.

It is in continuation of this that the Danish Data Protection Agency's assessment that the office community by not having introduced procedures prior to the inspection visit that ensures that emails containing confidential or sensitive personal information are sent using TLS encryption on the transport layer has violated Article 32 of the Data Protection Regulation.

The Danish Data Protection Agency must also note that the procedures that the office community has introduced after the inspection visit are assessed to be in accordance with Article 32 of the Data Protection Regulation, as according to the guidelines no e-mails containing confidential or sensitive personal information are sent to clients etc. without ensuring that TLS

encryption is used on the transport layer.

6. Conclusion

Following the audit of the office community, the Danish Data Protection Agency finds reason to conclude in summary:

That the office community - in accordance with Article 32 of the Data Protection Regulation - uses end-to-end encryption when exchanging S / MIME certificate over the tunnel mail community (hereinafter referred to as tunnel mail) for the transmission of confidential and sensitive personal information over the Internet to police, courts and other recipients the public tunnel list.

That the office community had not prior to the inspection visit introduced procedures that ensure that encryption is used on the transport layer via TLS for the transmission of confidential and sensitive personal information to clients, etc. over the Internet.

That the office community does not - in accordance with Article 5 (1) of the Data Protection Regulation 2, cf. Article 32 (1) (f) 1 and 2 - have demonstrated that they have prepared a risk assessment that addresses the risk associated with the transmission of confidential and sensitive personal data over the Internet, prior to the inspection visit.

That the office community is not aware of any cases where confidential or sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.

Overall, the Danish Data Protection Agency finds reason to criticize the fact that the office community has not complied with the requirements of the Data Protection Regulation in relation to points 2 and 3.