Supervision of treatment security at a law firm

Date: 05-11-2019

Decision

Private companies

Journal number 2019-41-0026

Summary

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

The Danish Data Protection Agency found that the law firm's processing of personal data in relation to the transmission of confidential and sensitive personal data via e-mail over the Internet was in accordance with the rules in the Data Protection Ordinance and the Danish Data Protection Agency's guidelines.

The Danish Data Protection Agency's concluding statement states, among other things, that the law firm uses end-to-end encryption with S / MIME certificates and forwarding with compulsory TLS 1.2 when the law firm sends e-mails with confidential and sensitive personal information to municipalities, companies, clients, relatives. , etc.

In addition, it appears from the statement that the law firm has demonstrated that it has prepared a risk assessment, in which a position is taken on the risk associated with the transmission of confidential and sensitive personal data over the Internet.

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

Decision

A law firm 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, the law firm in the spring of 2019 in connection with the inspection visit filled in a questionnaire and submitted this as well as additional material to the inspection. The inspection visit took place on April 8, 2019.

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

That the law firm - 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 to transmit confidential and sensitive personal information over the Internet to municipalities, companies and other recipients on the public tunnel list.

That the law firm - in accordance with Article 32 of the Data Protection Regulation - also uses encryption on the transport layer via forced TLS 1.2 for the transmission of confidential and sensitive personal data to clients and relatives etc. over the Internet.

That the law firm - in accordance with Article 5 (1) of the Data Protection Regulation 2, cf. Article 32 (1) (f) 1 and 2 - have shown that they have prepared a risk assessment, in which a decision is made on the risk associated with the transmission of confidential and sensitive personal data over the Internet.

That the law firm is not aware of any cases in which confidential or sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.

On that basis, the Danish Data Protection Agency considers the audit to be completed and does not take any further action on that occasion.

Below is a more detailed review of the Danish Data Protection Agency's conclusions.

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

Prior to the inspection visit, the law firm stated that the law firm sends confidential and sensitive personal information via e-mail over the Internet.

2. About the encryption solution

The law firm has stated that the encryption solution used works by sending all e-mail traffic through their data processor over a TLS 1.2 connection. Here, the traffic will pass through two layers. The first layer scans for viruses and spam, and the second layer tries to encrypt the email in the following order of priority:

Via tunnel mail to the recipient's domain so that the email is sent end-to-end encrypted.

It is examined whether the recipient has published an S / MIME certificate on the public tunnel mailing list, and in that case the e-mail is encrypted using the certificate in question.

It is being investigated whether the e-mail can be sent with encryption on the transport layer via a forced TLS 1.2 connection.

The law firm's data processor has also stated that a “secure recipients list” is also used - ie. a list of specific compatible

recipient domains - for which end-to-end encryption occurs automatically.

3. Emails to clients

The law firm has stated that communication with clients typically takes place by telephone and that e-mail correspondence with clients is very limited. To the extent that the law firm sends confidential or sensitive personal information to clients, the transmission is encrypted via a forced TLS 1.2 connection, if one is available. E-mails sent encrypted to clients are typically e-mails with order confirmation / price information / personal data policy, which may also contain information about the time of court hearings, etc.

The law firm has further stated that the law firm - in the rare case that an e-mail can not be sent encrypted to a client via the mentioned solution - makes a concrete assessment of whether the e-mail contains information that can be sent via ordinary e-mail. mail.

Finally, the law firm has stated that the law firm sends confidential and sensitive personal information by regular mail to clients who cannot receive encrypted email.

3.1. Summary

On the basis of what the law firm stated, the Danish Data Protection Agency assumes that the law firm uses compulsory TLS when e-mails containing confidential or sensitive personal information are sent to clients. The Danish Data Protection Agency thus finds that the law firm uses sufficient processing security when sending such e-mails.

4. Emails to other recipients

The law firm has stated that communication with the media, relatives and potential clients rarely takes place via e-mail, as the communication primarily takes place by telephone. To the extent that the law firm communicates with these recipients via e-mail, this is generally done via encrypted e-mail.

The law firm has also stated that the law firm communicates encrypted with the police and the court via tunnel email, just as it can sometimes happen that the law firm communicates directly with judges via tunnel email.

Finally, the law firm has stated that the law firm also sends emails via cell phone. During a staff meeting on 8 December 2018, the employees were informed that encrypted e-mail could now be sent via telephone within the organization as well as to other domains that have tunnel e-mail. The law firm has stated that the law firm therefore presupposes that the employees only send e-mails with confidential and sensitive personal information from the telephone if the recipient has tunnel e-mail.

4.1. Summary

On the basis of what the law firm stated, the Danish Data Protection Agency assumes that the law firm primarily communicates with the media, relatives and potential clients by telephone, and that if e-mail is used, it is encrypted.

Furthermore, based on the information provided by the law firm, the Danish Data Protection Agency assumes that the law firm uses end-to-end encryption with S / MIME certificates via tunnel mail when e-mails containing confidential or sensitive personal information are sent to professional actors, including the police, courts and others. recipients on the public tunnel list.

The Danish Data Protection Agency thus finds that the law firm uses sufficient processing security when sending such e-mails.

5. Cases where encryption has not been used

Prior to the inspection visit, the law firm has stated that since 1 January 2019, the law firm has used encryption in all cases when confidential and sensitive personal information is sent via e-mail over the Internet.

The law firm has added that the law firm has largely not sent anything over the Internet since 1 January 2019 that has not been encrypted, and that the law firm is not aware of cases where confidential or sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.

5.1. Summary

On the basis of what the law firm stated, the Danish Data Protection Agency assumes that the law firm is not aware of cases where confidential and sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.

6. Risk assessment

Prior to the audit visit, the law firm submitted a risk assessment to the audit dated 10 March 2019. The law firm has since - at the request of the Danish Data Protection Agency - submitted a version of the risk assessment, which was valid before the notification of the audit visit on 28 February 2019. of confidential and sensitive personal information over the Internet.

The law firm's risk assessment states that the risk associated with the transmission of confidential or sensitive personal information via e-mail is a means. The risk assessment also shows how this risk is reduced to an appropriate level by using tunnel mail or forced TLS if possible, and otherwise by assessing whether the e-mail can be sent with opportunistic TLS, or whether anonymisation or transmission should be used instead. by regular mail.

The law firm has also stated that the method for sending e-mails via secure mail has been reviewed at a staff meeting, that instructions are regularly sent to the staff about the use of encrypted e-mail, and that the law firm has an instruction that

employees must inform a particular consultant in the law firm whose confidential and sensitive information is sent unencrypted over the Internet.

6.1. Summary

It is the Data Inspectorate's assessment that the law firm, 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, in which a position is taken on the risk associated with the transmission of confidential and sensitive personal data over the Internet.

7. Conclusion

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

That the law firm - 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 to transmit confidential and sensitive personal information over the Internet to municipalities, companies and other recipients on the public tunnel list.

That the law firm - in accordance with Article 32 of the Data Protection Regulation - also uses encryption on the transport layer via forced TLS 1.2 for the transmission of confidential and sensitive personal data to clients and relatives etc. over the Internet.

That the law firm - in accordance with Article 5 (1) of the Data Protection Regulation 2, cf. Article 32 (1) (f) 1 and 2 - have shown that they have prepared a risk assessment, in which a decision is made on the risk associated with the transmission of confidential and sensitive personal data over the Internet.

That the law firm is not aware of any cases in which confidential or sensitive personal information has been sent unencrypted over the Internet since 1 January 2019.