Supervision of processing security at an audit firm

Date: 05-11-2019

Decision

Private companies

Journal number: 2019-41-0027

Summary

BDO Statsautoriseret revisionsaktieselskab (hereinafter BDO) was among the companies that the Danish Data Protection Agency had selected for supervision in 2019. Supervisors 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 BDO'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 Regulation and the Danish Data Protection Agency's guidelines.

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

In addition, it appears from the statement that BDO 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

BDO Statsautoriseret Revisionsaktieselskab (hereinafter BDO) 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, BDO filled out a questionnaire in the spring of 2019 in connection with the inspection visit and submitted this as well as additional material to the inspection. The inspection visit took place on April 9, 2019.

Following the inspection visit with BDO, the Danish Data Protection Agency finds reason to conclude:

That BDO - 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 data over the Internet to customers and other recipients in the public domain tunnel list.

That BDO - 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 customers over the Internet.

That BDO - 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 BDO is not aware of any cases where 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 conclusion.

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

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

BDO has stated that the company rarely sends personal information over the Internet in an audit context. However, the company has stated that it may happen that BDO in connection with tax advice sends confidential information in the form of tax returns containing e.g. social security numbers via e-mail over the Internet.

BDO has stated that the company communicates with its customers either via MIT BDO - which is a web platform on which documents are exchanged securely with BDO's customers - or via encrypted e-mail.

2. About the encryption solution

BDO has stated that the encryption solutions used are an attempt to encrypt e-mail in the following order of priority:

End-to-end encrypted via tunnel mail to the recipient's domain.

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.

Furthermore, BDO has stated that if none of the three solutions is possible, then the user is presented with an error message stating that the recipient does not support encryption and that the email will not be sent. From there, it is up to the individual employee's specific assessment whether the employee finds it necessary to encrypt the e-mail. If the employee deems it unnecessary to encrypt the email, the email will be forwarded using opportunistic TLS.

During the inspection visit and at the request of the Danish Data Protection Agency, BDO tried to send an e-mail with compulsory TLS to an e-mail server set up by the inspection, which does not support reception with TLS. As expected, and as confirmation of BDO's setup, the email in question could not be delivered.

BDO has stated that the company has chosen to use the encryption algorithm 3DES when sending via tunnel email, as several recipients do not support newer algorithms.

2.1. Summary

Based on the information provided by BDO, the Danish Data Protection Agency assumes that when BDO sends e-mails with confidential and sensitive personal information, BDO uses end-to-end encryption with S / MIME certificates to the extent possible and otherwise a forced TLS is used. 1.2 connection. The Danish Data Protection Agency thus finds that BDO uses sufficient processing security when sending such e-mails.

At the same time, the Danish Data Protection Agency encourages BDO to phase out the use of the algorithm 3DES, as the algorithm is not up-to-date. In this connection, the Danish Data Protection Agency should note that known vulnerabilities [1] in 3DES make the algorithm insecure in certain applications, but that e-mail is not covered by these applications. However, the Danish Data Protection Agency must nevertheless encourage BDO to phase out the use of 3DES, as the algorithm is not up-to-date and because safer alternatives are freely available.

3. Cases where encryption has not been used

BDO has stated that the company is not aware of cases where confidential or sensitive personal information has been sent unencrypted over the Internet since 1 January 2019. BDO has further stated that BDO has not received any feedback from employees that this should have occurred.

BDO has subsequently stated that the company has a procedure for how employees should act if confidential and sensitive

personal information is sent unencrypted over the Internet. The procedure prescribes that the employee must report such an incident to the IT security committee, which consists of several members of the management, including the meeting representatives, after which the committee assesses whether the incident must be reported to the Danish Data Protection Agency. BDO has sent a copy of the procedure to the Danish Data Protection Agency.

3.1. Summary

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

4. Risk assessment

Prior to the audit visit, BDO has submitted a risk assessment to the audit, which takes into account the transmission of confidential and sensitive personal data over the Internet.

BDO's risk assessment shows that there is a high weighted risk associated with the transmission of confidential or sensitive personal information via e-mail. The risk assessment also shows that this risk is reduced to an appropriate level by using the above-mentioned technologies, in particular end-to-end encryption whenever possible, and as a minimum by using TLS 1.2 encryption on the transport layer.

BDO has also prepared a guide for its employees regarding the use of encrypted e-mail, which is dated 12 December 2018.

Finally, BDO has stated that the departments for advisory and social auditing have carried out targeted training of employees in handling security breaches, just as BDO uses a number of e-learning videos targeted at employees about the use of encrypted e-mail, where management has the opportunity to check , what percentage of the videos the employees have seen, and that there has also been a follow-up test for the videos that each employee has had to complete.

4.1. Summary

It is the Data Inspectorate's assessment that BDO, 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.

5. Conclusion

Following the inspection visit with BDO, the Danish Data Protection Agency finds reason to conclude:

That BDO - 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 data over the Internet to customers and other recipients in the public domain tunnel list.

That BDO - 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 customers over the Internet.

That BDO - 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.

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

[1] See Bhargavan and Leurent On the Practical (In-) Security of 64-bit Block Ciphers (ACM CCS 2016) and NIST SP 800-57 Part 1 Revision 4 (Section 5.6.1)