Supervision of treatment security at the trade union

Date: 05-11-2019

Decision

Private companies

Journal number: 2019-41-0028

Summary

Kristelig Fagforening (hereinafter Krifa) 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.

In connection with the supervision, the Danish Data Protection Agency has expressed criticism that Krifa has not complied with the requirements of Articles 32 and 33 of the Data Protection Regulation.

The Danish Data Protection Agency's concluding statement states, among other things, that Krifa has violated Article 32 of the Data Protection Regulation by using the social security number of the person to whom the e-mail relates as the password for reading an e-mail stored on the company's secure web service for reading. of e-mail.

In addition, the statement states that Krifa has violated Articles 32 and 33 of the Data Protection Regulation by sending unencrypted e-mails in the period 1 January 2019 to 9 April 2019, where information about trade union affiliation could be deduced, and without having reported the incidents. to the Danish Data Protection Agency as a breach of personal data security.

The Danish Data Protection Agency has found grounds for issuing Krifa an order to cease using the personal identity number of the person to whom an e-mail for reading on the company's secure web service relates, as a password for reading the e-mail. The deadline for compliance with the order is 26 November 2019.

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

Decision

Kristelig Fagforening (hereinafter Krifa) was among the companies that the Danish Data Protection Agency had selected for inspection 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, Krifa 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 Krifa, the Danish Data Protection Agency finds reason to conclude:

That Krifa - in accordance with Article 32 of the Data Protection Regulation - uses certificate-based end-to-end encryption to the extent that the recipient supports it when Krifa submits e-mails containing confidential and sensitive personal information.

That Krifa - in accordance with Article 32 of the Data Protection Regulation - to the extent that the recipient does not support certificate-based end-to-end encryption, uses a solution called Secure @ Mail, which forwards end-to-end encryption to the data processor's server, after which TLS sends an notification email to the recipient, which contains a link to read the original email (after entering a password).

That Krifa - in accordance with Article 32 of the Data Protection Regulation - sends notification emails in connection with sending messages via Krifa Boks and Sikker @ Mail, as well as SMSs with passwords for reading e-mails on Sikker @ Mail server.

That Krifa has violated Article 32 of the Data Protection Regulation by using the social security number of the person to whom the e-mail relates as the password for reading Sikker @ Mail on the web server.

That Krifa has violated Articles 32 and 33 of the Data Protection Ordinance by sending unencrypted e-mails in the period 1 January 2019 to 9 April 2019, where information about trade union affiliation could be deduced, and without reporting the incidents to the Danish Data Protection Agency as a breach of personal data security .

That Krifa - 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.

Overall, the Danish Data Protection Agency finds reason to criticize the fact that Krifa has not complied with the requirements of the Data Protection Regulation in relation to points 4 and 5.

The Danish Data Protection Agency also finds grounds for ordering Krifa to cease using the personal identity number of the person to whom a Sikker @ Mail for reading on a web server relates, as a password for reading the e-mail. The order is issued

pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d.

The deadline for compliance with the order is 26 November 2019. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with. According to the Data Protection Act, section 41, subsection 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 d.

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, Krifa stated that the union sends confidential and sensitive personal information via e-mail over the Internet.

Krifa has stated that the union considers membership of Kristelig Fagforening as sensitive personal information, but that the union considers membership of Kristelig A-kasse or affiliation with Krifa (as a brand) as ordinary personal information.

2. About the encryption solution

Krifa has stated that when the union sends e-mails containing confidential or sensitive personal information, a solution called Safe @ Mail is used. The solution is integrated in Outlook, and all Krifa employees can use it.

When sending an e-mail via Secure @ Mail, the e-mail will be sent in one of the following ways in order of priority:

It examines whether the recipient domain is on a list of supported recipient domains (called the tunnel mailing list). If the recipient domain is on the tunnel mailing list, end-to-end encryption with a certificate issued by Nets takes place.

It is examined whether the recipient has a published and valid Nets issued OCES II company certificate, and in that case end-to-end encryption with that certificate is used.

It is examined whether the recipient has a published and valid Nets issued OCES II employee certificate, and in that case end-to-end encryption is used with the certificate in question.

If the recipient does not support end-to-end encryption with certificate (items 1-3 above), the email will be sent to a Secure @ Mail server at the data processor, where the email will be stored encrypted for 30 days. An notification email is then sent via opportunistic TLS to the recipient with a link to a web-based solution, where the email - after entering a password - can be read and downloaded.

In addition, Krifa uses a secure web-based system called Krifa Box, which is used when the union exchanges documents with

current and former members. With Krifa Boks, the union can place documents locally on a server, after which the current or former member will be sent a notification email with information that there is a new document for the person in Krifa Boks. Access to Krifa Boks takes place using NemID or with a combination of username and password.

Krifa has stated that the union in end-to-end encrypted transmission with certificate has chosen to use the encryption algorithm 3DES, as several recipients do not support newer algorithms.

2.1. Sending notification email

Krifa has stated that notification emails - both in connection with new documents in Krifa Box and in connection with sending e-mail to Sikker @ Mail server - are sent automatically via TLS 1.2 to Exchange Online. The notification email is then sent to the recipient via opportunistic TLS with the support of versions 1.0, 1.1 and 1.2. This means that Exchange Online encrypts the transport layer when sending these e-mails to the extent that the recipient supports reception via TLS, and that the e-mail is otherwise sent without encryption.

Krifa has stated that the content of a notification email depends on whether it has been sent in connection with a new document in Krifa Boks or in connection with a Sikker @ Mail e-mail.

Krifa has sent to the Danish Data Protection Agency examples of notification emails sent in connection with messages in resp. Krifa Box and Secure @ Mail.

If it is a notification email about a new e-mail in Sikker @ Mail, the notification email will include include an ID number on the e-mail, a link to read the e-mail (after which a password is required) and the subject field of the original e-mail. In the relevant example of a notification email sent in connection with a Secure @ Mail, the subject field is "FAG006-720-946". Krifa has stated that the subject field is the record number of a case that a member has with Krifa.

Krifa has generally stated about the allocation of journal numbers for cases in Krifa that there are three types of initial letter combinations, and that these are resp. "FAG", "AKS" and "VIR". The letter combination in question refers to which of Krifa's competence centers has created the case in question in the case processing system. This includes "FAG" legal professional case types and advice that have been set up in Krifa's legal centers or specialist centers. This can, for example, be cases with legal professional content (traditional trade union work) for members of the Christian Trade Union, as well as inquiry cases with legal professional content for persons who are only members of the Christian unemployment fund or neither members of the Christian unemployment fund nor the Christian Trade Union. The letter combination thus has no explicit connection with the

type of membership that recipients of the email have.

In the case of a notification email about a new document in Krifa Boks, both the notification field's subject field and body text will contain e.g. information about the name of the document. In addition, Krifa has stated that an advisory e-mail - via the name of the document in question - may contain information that there is news in a case, but may also contain information about, for example, a new information letter or receipt for e-mail.

Krifa has stated that advisory emails are also sent to non-members, and that in that case, as a starting point, these are emails to union representatives, employers or other similar professional actors.

2.2. Password for opening e-mails stored on Secure @ Mail server

Krifa has stated that when e-mail is sent, which is stored on the Secure @ Mail server (cf. point 4 above), it is basically the recipient's social security number that is used as the password.

Krifa has stated that the social security number has been chosen so that both the recipient and a possible third parties - eg a lawyer or employer - can access the e-mail and that the social security number works as a recognition method for both the member and the third party.

Krifa has also noted that the social security number is never stated, but that it is stated that the social security number is the password. The system supports the use of other passwords, which can be agreed ad hoc and which can be sent via SMS to the recipient. The text in question also appears from the subject field of the notification email in the SMS in question.

2.3. Summary

In connection with Krifa Boks, the Danish Data Protection Agency must note that it is only the notification emails that are sent in connection with new documents - and not Krifa Boks itself - that have been the subject of the inspection visit.

On the basis of what Krifa stated, the Danish Data Protection Agency can state that the subject field from an e-mail sent with Sikker @ Mail appears in both the notification email and in the SMS with password (if one is sent). Furthermore, the Danish Data Protection Agency can state that information about the document name appears in the notification email sent with a new document in Krifa Boks.

The Danish Data Protection Agency may also, on the basis of the information provided by Krifa, state that an advisory email from Krifa Boks may contain information that there is news in the recipient's case, and that the subject field of an e-mail sent via Sikker @ Mail may contain information about a case number .

Finally, the Danish Data Protection Agency can state that Krifa sends notification emails via opportunistic TLS without any guarantee that the content is encrypted and that text messages with passwords for reading e-mail on Sikker @ Mail server are sent unencrypted.

On the basis of what Krifa stated that a journal number with the introduction "FAG" does not mean that the recipient is a member of Kristelig Fagforening, the Danish Data Protection Agency assumes that it is not based on the journal number in the advisory email sent in connection with Sikker @ Mail the email is possible to deduce the recipient's union affiliation.

The Danish Data Protection Agency also finds that information that a person is a member of Krifa is not in itself a confidential or sensitive information. In this connection, the Danish Data Protection Agency has emphasized that Krifa is a collective term for two associations, Kristelig A-kasse and Kristelig Fagforening, and that it is possible to be a member of Kristelig A-kasse without being a member of Kristelig Fagforening. It is thus the Data Inspectorate's assessment that information that a person is a member of Krifa does not mean that the person in question has a trade union affiliation with the Christian Trade Union.

In addition, the Danish Data Protection Agency finds that the advisory emails in question, which have been submitted to the Danish Data Protection Agency, do not contain information from which it is possible to deduce trade union affiliations or information of a sensitive or confidential nature.

The Danish Data Protection Agency thus assumes that it is not possible to derive sensitive and confidential information from the sent notification emails from Krifa Boks, Sikker @ Mail and SMSs with a password for reading e-mail on Sikker @ Mail server.

When Krifa uses the procedure, where notification emails are sent via opportunistic TLS and SMS with a password for reading Secure @ Mail - potentially both are sent unencrypted - the confidentiality of the Secure @ Mail email in question depends on two accessing information, ie. the ID number (from the notification email) and the password (from the SMS). The Danish Data Protection Agency finds that Krifa has taken the necessary technical measures to ensure the confidentiality of the Sikker @ Mail in question, as unintentional access to it requires access to both the recipient's SMS and e-mail.

In summary, the Danish Data Protection Agency's assessment is that Krifa's sending notification emails and SMSs with passwords for reading Sikker @ Mail is in accordance with Article 32 (1) of the Data Protection Regulation. 1.

In relation to the fact that Krifa as a password for reading Sikker @ Mail on a web server by default uses the social security number of the person to whom the e-mail relates, it is the Data Inspectorate's opinion that Krifa must not base the

confidentiality of personal data processed on personal data per se. themselves, including by, for example, using the social security number as an access factor to the registered information.

The Danish Data Protection Agency has emphasized that a date of birth is ordinary, non-sensitive personal data, which will often be known by others than the data subject, that the assignment of a social security number follows a publicly known method by which the possible social security numbers for a given date of birth can is limited to a small number of options, and that a social security number is used widely across authorities, etc., which entails a high probability - and thus an increased risk - that the confidentiality of the information that the access control must ensure is compromised.

Against this background, the Danish Data Protection Agency's assessment is that Krifa has not implemented appropriate security measures, as required by Article 32 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency also calls on Krifa to phase out the use of the 3DES algorithm, 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 urge Krifa 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

Prior to the inspection visit, Krifa has stated that the trade union has known of four cases since 1 January 2019, in which e-mails - from which information about trade union affiliation can be deduced - have been sent without the desired encryption. This means that the e-mails in question are sent with opportunistic TLS rather than using Krifa Boks or Sikker @ Mail. Krifa has stated that the e-mails in question, after investigation, have been found to have been sent with TLS 1.2 for the first jump.

Krifa has further stated that in the period 1 January to 28 February 2019 - due to an error where the word "Trade union" appeared in the body text instead of "Krifa" - 1,544 notification emails were sent via opportunistic TLS, of which information on trade union affiliation may possibly be inferred.

Krifa has stated that the incidents have not been reported to the Danish Data Protection Agency in accordance with Article 33 of the Data Protection Regulation. Krifa has stated that this has not been done on the basis of an assessment of whether Krifa is sure that the e-mail is addressed to the correct recipient. whether the recipient is a private person or professional actor.

Furthermore, Krifa has stated that the assessment takes into account that the e-mails in question were sent with opportunistic

TLS, and that the union's statistics for March 2019 show that TLS was used for at least 99.74% of the e-mails sent.

3.1. Summary

Based on the information provided by Krifa, the Danish Data Protection Agency assumes that the trade union has since 1 January 2019 documented two categories of incidents in which e-mails with sensitive personal information have been sent unencrypted.

Against this background, the Danish Data Protection Agency's assessment is that Krifa has not implemented appropriate security measures as required by Article 32 of the Data Protection Regulation.

It is also the Data Inspectorate's assessment that the breaches of personal data security in question should have been reported to the Authority, cf. Article 33 of the Data Protection Regulation.

In this connection, the Danish Data Protection Agency has emphasized that - contrary to the Authority's practice and Krifa's own guidelines and risk assessment - unencrypted e-mails have been sent with sensitive personal data, which is why a risk to the data subjects' rights and freedoms must be expected in connection with the concrete events.

4. Risk assessment

The Danish Data Protection Agency has noted that prior to the audit visit, Krifa has submitted a written risk assessment to the audit dated 20 December 2018, which focuses on the transmission of confidential and sensitive personal information over the Internet.

The Danish Data Protection Agency has noted that the risk assessment is based on 8-12 main parameters, where a specific valuation has been made of each individual risk associated with the processing of personal data.

4.1. Summary

It is the Data Inspectorate's assessment that Krifa, 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 Krifa, the Danish Data Protection Agency finds reason to conclude:

That Krifa - in accordance with Article 32 of the Data Protection Regulation - uses certificate-based end-to-end encryption to the extent that the recipient supports it when Krifa submits e-mails containing confidential and sensitive personal information.

That Krifa - in accordance with Article 32 of the Data Protection Regulation - to the extent that the recipient does not support certificate-based end-to-end encryption, uses a solution called Secure @ Mail, which forwards end-to-end encrypted to the data processor's server, after which TLS sends an notification email to the recipient, which contains a link to read the original email (after entering a password).

That Krifa - in accordance with Article 32 of the Data Protection Regulation - sends notification emails in connection with sending messages via Krifa Box and Sikker @ Mail, as well as SMSs with passwords for reading e-mails on Sikker @ Mail server.

That Krifa has violated Article 32 of the Data Protection Regulation by using the social security number of the person to whom the e-mail relates as the password for reading Sikker @ Mail on the web server.

That Krifa has violated Articles 32 and 33 of the Data Protection Regulation by sending unencrypted e-mails in the period 1 January 2019 to 9 April 2019, where information about trade union affiliation could be deduced, and without reporting the incidents to the Danish Data Protection Agency as a breach of personal data security .

That Krifa - 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.

Overall, the Danish Data Protection Agency finds reason to express criticism that Krifa has not complied with the requirements of the Data Protection Regulation in relation to points 4 and 5.

The Danish Data Protection Agency must also issue an order to Krifa to cease using the personal identity number of the person to whom a Sikker @ Mail for reading on a web server relates, as a password for reading the e-mail. The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d. According to the Data Protection Act § 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 d.

6. Concluding remarks

The Danish Data Protection Agency notes that in relation to the security breaches concerning the transmission of the 1,544 notification emails, the Danish Data Protection Agency has taken a position on the incident in connection with this supervisory case. On this basis, Krifa must not report the security breaches to the Danish Data Protection Agency.

The Danish Data Protection Agency is then awaiting confirmation from Krifa that the order has been complied with. The confirmation must be received by the Danish Data Protection Agency no later than 26 November 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)