DATATILSYNET

Danish Agro A.M.B.A
Køgevej 55
4653 Karise
Danmark

Sendt med Digital Post

26 October 2021

J.No. 2021-7329-0005
Doc.no. 399491
Caseworker
[redacted]

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

Notification of personal data breaches

The Danish Data Protection Agency will return to the case where Danish Agro A.M.B.A. on 20 April 2020 reported a personal data breach. The notification has the following reference number:

16ef760166c5a375e2a7c141dfe12e9dc320c5c4.

1. Decision

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for **issuing a reprimand** that Danish Agro A.M.B.A's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the General Data Protection Regulation.

Furthermore, The Danish Data Protection Agency finds no basis for concluding that Danish Agro A.M.B.A's processing of personal data has taken place in breach of the rules laid down in Article 34(1) of the GDPR.

Below is a detailed examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Statement of the facts

Danish Agro A.M.B.A reported a personal data breach on 20 April 2020.

Danish Agro A.M.B.A subsequently sent a follow-up to the Danish Data Protection Agency on 28 April 2020.

On 5 May 2020, the Danish Data Protection Agency sent a hearing, which Danish Agro A.M.B.A replied to on 20 May 2020.

According to the information in the case, one of Danish Agro A.M.B.A's employees has been subjected to a phishing attack on 10 April 2020, where a click on a link from a compromised business connection resulted in hackers having access to Danish Agro A.M.B.A's networks and servers in the period from 11 April and 19 April 2020, including personal data stored in a number of IT systems, pay systems, and customer systems. Hackers had encrypted the data accessed, resulting in loss of availability and confidentiality of personal data.

Personal data was stored centrally in its own data centre in Denmark, and the incident involved employees in Denmark, Norway, Sweden, Finland, Estonia, Latvia and Poland.

2,1. Comments by Danish Agro A.M.B.A

Danish Agro A.M.B.A has stated that personal data about 5000 current and 2500 former employees including name, email, work phone, possibly user names and passwords were accessed. The hackers targeted business information for blackmail and not for employees' personal data.

[redacted]

Prior to the incident, Danish Agro A.M.B.A has reminded and continuously informed employees about the safe handling of emails.

It is Danish Agro A.M.B.A's assessment that the breach does not pose a threat to the rights or freedoms of the registrars. Danish Agro A.M.B.A has emphasised the nature of the information covered and that user access for the company's current employees has been reset and changed.

As regards the notification of data subjects, Danish Agro A.M.B.A has stated that information has been provided on the Danish Agro A.M.B.A's website. In addition, on 21 April 2020, the existing 5000 employees were informed about the event, focusing on the practical challenges that the event posed to the individual employees and the actions that had been taken. On May 1, 2020, pursuant to Article 34 of the GDPR, it was announced to all employees that hackers have been searching for information such as social security numbers and banking information, and that a mapping of the attack shows that hackers have only accessed information about work related names, phone numbers and email addresses. In this connection, instructions have been given about caution and how the employees should behave, as well as an explanation of how far in the process of handling the incident Danish Agro A.M.B.A is.

No personal data about customers has been accessed and therefore no notification has been made of them.

3. Reasons for the decision of the Danish Data Protection Agency

The Danish Data Protection Agency assumes that a member of Danish Agro A.M.B.A's employees on 10 April 2020 has been subjected to a phishing attack which resulted in hackers having access to Danish Agro A.M.B.A's networks and servers, including personal data stored in a number of IT systems, pay systems, and customer systems during the period from 11 April to 19 April 2020.

The Danish Data Protection Agency thus assumes that there has been an unauthorised transfer of personal data, which is why it considers that there has been a breach of personal data security in accordance with Article 4(12) of the General Data Protection Regulation.

3.1. It follows from Article 32(1) of the General Data Protection Regulation that the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risks inherent in the processing of personal data by the controller.

The controller thus has an obligation to identify the risks posed by the data subject's processing and to ensure that appropriate security measures are put in place to protect data subjects from those risks.

Following an examination of the case, the Danish Data Protection Agency considers that Danish Agro A.M.B.A's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

The Data Protection Agency concurs with Danish Agro A.M.B.A's own assessment that further technical and organisational measures were needed to ensure an appropriate level of security.

The Danish Data Protection Agency has also laid emphasis to the fact that Danish Agro A.M.B.A's has implemented these new measures, [redacted].

The Danish data Protection Agency therefore considers that there are grounds for issuing a reprimand that Danish Agro A.M.B.A's processing of personal data originally was not carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

The Danish Data Protection Agency has noted that prior to the incident Danish Agro A.M.B.A has reminded and continuously informed the employees about the safe handling of emails.

3.2. It follows from Article 34(1) of the Regulation that where a breach of personal data security is likely to present a high risk to the rights and freedoms of natural persons, the controller shall, without undue delay, inform the data subject of the personal data breach.

The Danish Data Protection Agency finds no basis for concluding that Danish Agro A.M.B.A's processing of personal data has taken place in breach of the rules laid down in Article 34(1) of the GDPR.

Furthermore, the Danish Data Protection Agency finds no grounds for disavowing Danish Agro A.M.B.A's assessment that there should be no notification to customers as no customer information has been accessed.

4. Final remarks

The Danish Data Protection Agency regrets the lengthy processing time due to the cross-border nature of the case and the great busyness of the supervision.

The Danish Data Protection Agency should note that Danish Agro A.M.B.A as data controller could consider installing protection on employees equipment that prevents the execution of programs etc. The supervision shall also point to the possibility of restricting the rights of each employee on the local machine, so that the code could not be run without separate approval.

The Danish Data Protection Agency's decision may be appealed to the courts.

The Danish Data Protection Agency thus considers the case closed and does not proceed further in the case.

Kind regards

[redacted]

Annexes: Legal basis.

Annexes: Legal basis

Extracts from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 2 (1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 32 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data; 4.5.2016 L 119/51 Official Journal of the European Union EN
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3.Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4.The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3.The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. 5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. 4.5.2016 L 119/52 Official Journal of the European Union EN

2.The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3.The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.