DATATILSYNET

Danske Bank A/S
Holmens Kanal 2-12
1092 København K

Sendt via Digital Post til CVR 61126228

13 June 2022

J.No. 2021-442-12980
IMI case no. 483097
Caseworker
Betty Husted

Regarding personal data breach, your case no. INC000003185717

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

VAT No. 11883729

The Danish Data Protection Agency hereby returns to the case where Danske Bank A/S has notified a personal data breach to the Danish Data Protection Agency on 12 May 2021.

1. Decision

After examining the case, the Danish Data Protection Agency considers that there are grounds for issuing a **reprimand** that Danske Bank's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

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

2. Summary of facts

Danske Bank notified a personal data breach to the Danish Data Protection Agency on 12 May 2021.

According to the notification, a technical error in sending 132 electronic invoices containing the name, address and invoice number to Danske Bank's customers in Finland resulted in the 132 invoices being searchable and visible to 14.511 Finnish business customers in the period between 5 May 2021 and 10 May 2021.

The breach occurred due to a technical error in which 132 invoices were placed in the 'District platform' system without the recipients' account details. The blank receiver field allowed these invoices to be searched if the user performed a search without entering receiver's information (a blank search).

Danske Bank's investigation of the breach shows that 371 Finnish users accessed the electronic invoices between 5 May 2021 and 10 May 2021. However, the number of users who performed a search without entering the receiver's information (a blank search) would most likely be lower.

District Platform is an application developed by Danske Bank for the bank's business customers to search for invoices, among other things.

Danske Bank stated that on 10 May 2021, recipient information was added manually to the 132 electronic invoices. On 20 May 2021, a safety mechanism was verified and released ensuring the possibility of performing a search for electronic invoices with no receiver information was disabled.

3. Reasons for the Danish Data Protection Agency's decision

On the basis of the information provided by Danske Bank, the Danish Data Protection Agency considers that from 5 May 2021 to 10 May 2021 it has been possible for the bank's business customers in Finland to see unrelated invoices.

According to Article 32(1) of the GDPR the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risks posed by the processing of personal data by the controller.

There is thus an obligation on the controller to identify the risks that the controller's processing poses to data subjects and to ensure that appropriate safeguards are put in place to protect data subjects from those risks.

The Data Protection Agency is of the opinion that the requirement under Article 32 on adequate security will normally imply **that** in systems with a large number of confidential information about a large number of users, higher requirements must be imposed on the controller's carefulness in ensuring that there is no unauthorised access to personal data, **that** all likely outcomes should be tested in the context of the development of software where personal data are processed and **that** a relevant security measure in Article 32(1)(d) specifically mentions that the controller implements a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure security of processing.

In the light of the above, the Danish Data Protection Agency considers that Danske Bank – by not having continuously tested the Bank's technical measures – has not taken appropriate organisational and technical measures to ensure a level of security appropriate to the risks associated with the processing of personal data by Danske Bank, cf. Article 32(1) of the GDPR.

After examining the case, the Danish Data Protection Agency considers that there are grounds for issuing a **reprimand** that Danske Bank's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

As a mitigating fact, the Danish Data Protection Agency has taken into account that the breach concerned only information on name, address and invoice number.

Kind regards

Betty Husted