

## Reports of breaches of personal data security at PFA Pension

Date: 16-05-2019

Decision

Private companies

On the basis of a number of notifications of breaches of personal data security from PFA Pension, the Danish Data Protection Agency took up a case of its own motion and is now criticizing.

Journal number: 2019-431-0021

Summary

On the basis that PFA Pension per. On 8 February 2019, having reported 66 breaches of personal data security to the Danish Data Protection Agency, the Danish Data Protection Agency started a case against PFA Pension on its own initiative. By decision of 16 May, the Danish Data Protection Agency criticizes the fact that PFA Pension's processing of personal data has not taken place in accordance with the rules in Article 32 of the Data Protection Regulation.

After a closer examination of the notifications received, the Danish Data Protection Agency has found that 62 out of 66 notifications relate to unintentional disclosure of personal data in connection with the transmission of documents via the communication solution "My PFA", e-Box, by letter or similar. PFA Pension has stated that the 66 breaches of personal data security constitute a relatively small proportion of the total communication with the company's customers, but that the number is nevertheless too high. PFA Pension has stated that approximately 270,000 customers annually receive electronic or physical answers from PFA Pension as a result of their inquiry, and that the reported breaches of personal data security only relate to 0.3 per mille of the total communication with the company's customers.

Despite the Data Inspectorate's criticism of PFA Pension, the Authority also notes that PFA Pension continuously monitors the established security level and that the company took steps to implement further security measures to strengthen processing security, based on the breaches that have already occurred.

Decision

The Danish Data Protection Agency hereby returns to the case where the Authority has requested PFA Pension for an opinion in connection with the company per. February 8, 2019 has reported 66 breaches of personal data security to the Authority, in particular regarding unintentional disclosure of personal data.

## Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that PFA Pension's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation [1]. 1.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

### 2. Circumstances of the case

After a review of the notifications of breaches of personal data security received by the Danish Data Protection Agency, the Authority has been able to establish that PFA Pension per. February 8, 2019 has reported 66 breaches of personal data security to the Authority.

Based on a closer examination of the notifications received, the Danish Data Protection Agency has been able to establish that 62 out of 66 notifications relate to unintentional disclosure of personal data in connection with the transmission of documents via the communication solution "My PFA", e-Box, by letter or similar.

In response to the Danish Data Protection Agency's request of 18 February 2019, PFA Pension issued a statement on 4 March 2019 regarding the reported breaches of personal data security.

PFA Pension has generally stated that the 66 breaches of personal data security regarding unintentional disclosure of customers' personal information - in PFA Pension's own opinion - constitute a relatively small proportion of the total communication with the company's customers, but that the number is nevertheless too high.

PFA Pension has stated that around 270,000 customers annually receive electronic or physical answers from PFA Pension as a result of their inquiry, and that the reported breaches of personal data security only relate to 0.3 per mille of the total communication with the company's customers.

PFA Pension has also stated that the number of breaches of personal data security as a result of unintentional disclosure is divided into 36 unintentional disclosures via the communication solution My PFA, 17 unintentional disclosures via postal mail and 13 unintentional disclosures using other communication solutions (e-signature solutions -mail, e-Box, upload to the Board of Appeal portal and information sent via bank). Four of the unintentional transfers via letter mail took place in connection with PFA Pension's response to requests for insight.

In addition, PFA Pension has stated that the company on 7 February 2019 - as a result of the breaches of personal data

security - decided to introduce additional control measures when communicating with customers via My PFA, after which employees must actively "check" that the attached document has been checked for right recipient before dispatch. PFA Pension's used module letters via Word will also be integrated with the customer communication via My PFA in order to ensure that the message and document are addressed to the same customer. PFA Pension expects that these measures, which are expected to be implemented before the end of April 2019, will significantly reduce the number of breaches of personal data security.

In responding to requests for insight by letter post, PFA Pension has emphasized to the employees the existing requirement for "partner control"; that is, a colleague must check the shipment before the documents are sent. Following the tightening, the company has not found any further breaches of personal data security in this process.

PFA Pension has subsequently stated that the company handles physical shipments by automatic enveloping, which helps to minimize the risk of customer letters containing personal information about others than the person for whom the letter is intended. Despite automatic enveloping, a significant number of physical shipments are also packed manually by employees (approximately 82,500 annually). PFA Pension has emphasized that employees must be careful when packing letters.

In addition, PFA Pension has stated that in connection with the implementation of the data protection regulation, the company has prepared policies, business procedures and workflows and conducted training in the business areas in order for employees to become familiar with the data protection rules, including how personal data is handled and communicated. safe with customers. All PFA Pension employees must complete an e-learning course annually, and in the next course it will be emphasized that the employees must be careful in relation to ensuring that material is sent to the right recipient, just as the course is supplemented with examples of breaches of personal data security. , which employees must pay special attention to. Finally, PFA Pension has stated that all employees have access to the company's current policies, business procedures and workflows regarding data protection.

#### Justification for the Danish Data Protection Agency's decision

The Danish Data Protection Agency finds that PFA Pension's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. 1.

In this connection, the Danish Data Protection Agency has emphasized in particular that in the period from 25 May 2018 to 8 February 2019, PFA Pension has reported 66 breaches of personal data security to the Authority, where PFA Pension has by

mistake passed on personal information about customers to incorrect recipients, of which the unintentional disclosure in 62 of the cases has taken place by attaching the wrong document (s) or sending documents to the wrong recipient in connection with sending via the communication solution "My PFA", e-Box, by letter post or similar.

The Danish Data Protection Agency has also emphasized PFA Pension's own assessment that the number of breaches of personal data security is too high and that the company has been able to introduce further relatively less technical and organizational measures in order to ensure a more appropriate level of security.

In doing so, the Danish Data Protection Agency has emphasized that PFA Pension has taken these new measures, including e.g. in relation to the communication solution My PFA, where the employee must confirm that the attached document has been checked for the correct recipient before sending, just as the company's used module letters via Word will technically be integrated with customer communication via My PFA in order to ensure message and document to the same person.

In addition, the Danish Data Protection Agency has emphasized that PFA Pension intends to take further measures in relation to teaching employees, including adapting the company's e-learning material so that it is emphasized that employees must be careful in relation to ensuring that material is sent correctly. recipient.

While the Danish Data Protection Agency, in the light of the breaches of personal data security, finds that there are grounds for expressing criticism that PFA Pension's processing of personal data has not taken place in accordance with Article 32 (1) of the Regulation. 1, however, the Authority has similarly noted that PFA Pension continuously monitors the established security level, and that the company, on the basis of the breaches passed, already before the Authority's inquiry took steps to implement additional security measures to strengthen treatment security.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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).