The Danish Data Protection Authority expresses serious criticism of the Danish Financial Supervisory Authority's processing of personal data

Date: 21-04-2022

Decision

Public authorities

Serious criticism

Reported breach of personal data security

Unintentional disclosure

Treatment safety

The Danish Data Protection Authority expresses serious criticism of the Danish Financial Supervisory Authority for not having met the requirement for adequate security, when the Danish Financial Supervisory Authority inadvertently provided information about whistleblowers to a journalist.

Journal Number: 2020-442-8099

Summary

The Danish Data Protection Authority has made a decision in a case where the Danish FSA inadvertently passed on information about whistleblowers to a journalist in connection with a request for access to documents. The accidental disclosure occurred because the FSA had not removed personal data in a sufficiently secure manner from the material that had been given access to. The FSA had thus crossed out personal data in the provided PDF documents in order to exclude them from the material, but the information could be read by "hold the mouse cursor" on crossed-out passages.

It appears from the case that the Danish Financial Supervisory Authority was not aware that it is necessary to delete the hidden information behind the displayed document (metadata, etc.), to ensure that it will no longer be possible to find it.

Lack of technical and organizational measures

When assessing the case, the Danish Data Protection Authority, among other things, emphasis that the requirement for adequate security implies that the data controller must establish measures to ensure that material that is passed on does not contain personal data that should have been anonymised.

In addition, the Danish Data Protection Authority has placed particular emphasis on the fact that the risk to the data subject's

rights must generally be considered higher when the information originates from a whistleblower scheme, just as the Danish Data Protection Authority found that it is a generally known part of the functionality of programs that are technically used for strikeout, that metadata information or underlying layers of information can be found after strikeout.

Against this background, the Danish Data Protection Authority expressed serious criticism of the Danish Financial Supervisory Authority's processing of personal data, as this has not been done in accordance with the rules in the data protection regulation.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that the Danish Financial Supervisory Authority's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

It appears from the case that the FSA received a request for access to documents from a journalist regarding access to the inquiries that the FSA had received via the FSA's whistleblower mailbox, which concerned good practice for financial companies in 2019 and 2020.

In addition, the Danish FSA has stated that access to documents was granted in accordance with the Public Disclosures Act, and that information that could identify the persons in question who had contacted the Danish FSA's whistleblower mailbox was excluded from the documents. The document inspection was announced on 31 May 2020.

On Saturday 6 June 2020, the FSA was contacted via e-mail by one of the persons who had reported an inquiry to the FSA. The person stated that the person concerned had been contacted regarding the inquiry to the Danish Financial Supervisory Authority via e-mail by the journalist who had sought access to documents. The Danish Financial Supervisory Authority became aware of the breach when the email was read on Monday 8 June 2020.

The Danish Financial Supervisory Authority then contacted the journalist, who stated that he could find the information about the email address by holding the marker (cursor) over places in the pdf document, which were immediately anonymized by black crossing. The places during the anonymization where there was an underlying link or email address could thus be seen by the journalist by holding the marker (cursor) over the black line. In this way, the journalist had obtained information about

the email address.

The supplied material has been reviewed by the Danish Financial Supervisory Authority, which has been able to establish that the email addresses of seven people who have sent inquiries to the Danish Financial Supervisory Authority's whistleblower mailbox can be found.

The Danish Financial Supervisory Authority's work description for handling file access cases, which was in force at the time of the breach of personal data security, contained a section on extracting information. Among other things, the following appeared from the section:

"In practice, the extraction of information will be done by the case manager crossing out everything that is not covered by the extraction obligation".

In addition, the Danish Financial Supervisory Authority has stated that the job description must be seen in the context of regular training for assistants when new employees process requests for access to documents at the Danish Financial Supervisory Authority. The most widespread method of anonymisation in the Danish Financial Supervisory Authority has in practice been to cross out with a marker, after which the document was scanned. An alternative option has been to replace the information that had to be anonymised with X's.

The FSA has stated that it was the FSA's opinion before the data breach of 31 May 2020 that the job description for processing file access cases was adequate. In this connection, the FSA has stated that the FSA has not previously had incidents where insufficient anonymisation has led to a breach of personal data security. Since the breach, the Danish Financial Supervisory Authority has updated the job description for handling document access requests.

The Danish FSA has also stated that the material to which access has been granted should have been scanned as a PDF file after anonymisation prior to transmission. In this way, it would not have been possible to become familiar with the personal data, which immediately appeared to be anonymised. The error that led to the journalist having access to the exempted information was due to the FSA not being aware that it is possible to find information about e.g. email addresses and other underlying links by holding the marker (cursor) over places in a pdf document, which is immediately anonymized by black strikethrough. The Danish Financial Supervisory Authority was thus not aware that it is necessary to delete the hidden information behind the displayed document (metadata etc.) to ensure that it will no longer be possible to find it.

3. Reason for the Data Protection Authority's decision

It follows from the data protection regulation, article 32, subsection 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the data controller's processing of personal data.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects against these risks.

The Danish Data Protection Authority is of the opinion that the requirement in Article 32 for adequate security implies that the authority or company responsible for the data must establish appropriate measures to ensure that material that is passed on does not contain personal data that should have been anonymised. In this regard, it is essential that the extraction method chosen cannot be easily bypassed, or masking removed with standardized tools. It is therefore the Danish Data Protection Authority's opinion that a technical solution must not leave traces of the removed personal data, not even in metadata. A data controller must therefore be fully aware of the functionality of the program that is used, and give the necessary instructions to the employees, which ensures that the "layers" in the document that contain personal data - which must be excluded - are effectively removed.

Additional measures that – depending on the circumstances – may constitute an appropriate measure can e.g. be a requirement for a manual physical deletion based on prior review of the material on the basis of clear instructions from the data controller, if applicable. combined with a scanning tool.

The Danish Data Protection Authority assumes that personal data had been crossed out in the material to which insight had been given in order to exclude this, but that the information could be read by "holding the mouse cursor" on crossed out passages. In addition, the Danish FSA - based on what the FSA itself explained - assumes that the FSA was not aware that it was possible to view the information in this way.

It is the Danish Data Protection Authority's opinion that the Danish FSA had not implemented appropriate technical and organizational measures prior to the breach, as the Danish FSA did not have sufficient procedures for anonymising information in connection with file access requests.

The Danish Data Protection Authority has emphasized that the Danish Financial Supervisory Authority did not have the necessary clear and precise instructions for the anonymisation of personal data in relation to document inspection requests, etc., and that the FSA did not have the necessary understanding of which methods must be implemented to delete - also - the

hidden information that is behind the strikethrough in the displayed document (metadata, etc.), to ensure that the personal data does not longer will be found.

It is the Danish Data Protection Authority's assessment that a job description that only stipulates that case handlers must cross out everything that is not covered by the extraction obligation is not precise enough to provide sufficient security for correct anonymisation. Especially not in relation to the - in this case - chosen technical solution. The fact that, in addition, employees were trained in a safe work process by sidekick training does not change the need for clear and precise instructions on correct anonymisation. The Danish Data Protection Authority has placed particular emphasis on the fact that the risk to the data subject's rights must generally be considered higher when the information has been received via a whistleblower scheme. The Danish Data Protection Authority notes that it is a generally known part of the functionality in programs that are technically used for strike-through that metadata information or underlying layers of information can be found after strike-through. In view of this and as the Danish FSA was not aware that it is necessary to delete the hidden information behind the displayed document (metadata etc.) to ensure that it will no longer be possible to find it, bystander training cannot ensure sufficient security.

Based on this, the Danish Data Protection Authority finds that the Danish Financial Supervisory Authority has not taken appropriate organizational and technical measures to ensure a level of security that matches the risks involved in the Danish Financial Supervisory Authority's processing of personal data, cf. the Data Protection Regulation, Article 32, subsection 1.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that the Danish Financial Supervisory Authority's processing of personal data has not taken place in accordance with the rules in the Data Protection Regulation, Article 32, subsection 1.

When choosing a sanction, the Danish Data Protection Authority emphasized the fact that the information was from a whistleblower scheme, where the disclosure of information requires special attention from the data controller. The Norwegian Data Protection Authority has placed special emphasis on the long case processing time at the Norwegian Data Protection Authority.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).