The Digital Agency is criticized for not having adequate security

Date: 04-03-2022

Decision

Public authorities

Criticism

Reported breach of personal data security

Unauthorized access

Treatment safety

By mistake, the Digital Agency gave 26 curators access to the digital mailboxes of the wrong companies. The Norwegian Data Protection Authority expresses criticism in this decision, which emphasizes that it is not enough to base your security on the fact that human errors have not occurred in the past.

Journal number: 2021-442-12425

Summary

The Danish Data Protection Authority has expressed criticism in a case where the Digital Agency had reported a breach of personal data security to the Danish Data Protection Authority.

The Danish Agency for Digitization mistakenly gave 26 curators access to the digital mailboxes of the wrong companies. The error was probably due to the fact that the lines with cvr numbers had been shifted on the list the agency had sent to their supplier e-Boks.

During the processing of the case, the Digital Agency claimed that the agency had not previously experienced that errors had occurred in the preparation of the list in question. After the incident, the agency introduced a procedure where an additional employee reviews the lists for errors before they are sent to the supplier, in order to minimize the risk of errors.

The Danish Data Protection Authority found that, by not having introduced measures to ensure that the lists were correct, and - according to what has been reported - by solely basing the security on the fact that no human errors had previously occurred - it had not met the rules with treatment safety.

The decision is interesting because it shows that it is not enough to base one's safety on the fact that human errors have not previously occurred, as it is generally known that human errors do occur, which is why safety cannot - alone - be based on a

belief so that people do not make mistakes.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that the Digital Agency'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

On 31 March 2021, the Digital Agency reported a breach of personal data security to the Danish Data Protection Authority.

It appears from the notification that on 29 and 30 March 2021, the Digital Agency was contacted by a law firm regarding unlawful access to a company's digital mailbox. The law firm, as curator, had requested the Danish Agency for Digitalisation to gain access to another company's digital mailbox. However, the law firm discovered that they had gained access to the wrong company mailbox, and they then contacted the Danish Agency for Digitalisation.

It also appears from the report that, following the inquiry from the law firm, the Agency for Digital Marketing contacted the agency's supplier, e-Boks, and asked them to close the unlawful access on 30 March 2021. e-Boks confirmed that the access had been closed on 30 March 2021 .On the basis of the specific request, the Digital Agency carried out a closer investigation on 31 March 2021, which showed that a further 25 incorrect accesses had been given.

The Agency for Digitization has stated that the agency is data responsible for the allocation of curator access to company mailboxes in Digital Post. As the responsible authority for the joint public digital gateway solution "Digital Post", the Digitalization Agency handles the work of assigning read access to companies' digital mailboxes in the event of bankruptcy, termination, etc. By contacting the Danish Agency for Digitalisation, the trustee or liquidator can request access to the company's digital mailbox, if you can document a rightful access to the mailbox in question.

It appears from the Digitalisation Agency's statement to the Danish Data Protection Authority that, in the specific incident, the agency's further investigations have revealed that the error arose because the access holder (the person/legal entity who requests read access to a company mailbox) and the access provider (the person who must is given mailbox reading access to) had been compiled incorrectly on the basis of a list of 25 March 2021 that the agency had drawn up and subsequently sent to the supplier e-Boks.

The Digital Agency has argued that the erroneous allocation probably occurred because the lines with cvr numbers have been shifted, so that the cvr numbers of the access holder and the access provider have been put together incorrectly in the forwarded list. On the basis of this list, the agency's supplier e-Boks created the technical access, as neither the agency nor e-Boks were aware at the time that there were errors in the list in question.

In addition, the Digitalization Agency has stated that the agency prepares three lists each week, depending on the type of company that is given access to, as well as the company's status in the cvr register. This is a manual process which consists of several different steps, and it is the agency's assumption that the error occurred in one of the last steps in the preparation of this list. The board's investigation has also pointed out that the error occurred in connection with the manual part of the process.

The Danish Agency for Digitization has also stated that the agency has not previously experienced that errors have occurred in the preparation of the list in question. The list where the security incident happened and where the cvr numbers were compiled incorrectly was not part of the multi-eye principle at the time.

In this connection, the Digital Agency has stated that this multi-eye principle is currently implemented on all three lists, so that the risk of errors is minimised.

In continuation of this, the Digitalization Agency has stated that the agency has implemented a number of measures to minimize the risk of this type of security incident occurring. The Danish Agency for Digitalisation has, among other things, introduced a procedure where an additional employee reviews the lists for errors before they are sent to the supplier. In addition, the Agency has noted that the list where the security incident in question occurred was not covered by this procedure at that time, as the Agency had not previously experienced problems with this specific list. Which was the reason why the error was not detected by the other employee.

In addition, the Digitalization Agency has stated that when the agency became aware of the security incident, they ordered log files from the supplier e-Boks. The logs showed that none of the 26 incorrectly assigned accesses had been used. The law firm, which alerted the agency to the security incident, has also confirmed in writing to the agency on 31 March 2021 that the law firm has not accessed the contents of the company mailbox to which they had mistakenly gained access.

The Digital Agency has stated that it is the agency's assessment that the other 25 wrongly assigned company accesses and those registered (as well as the personal data appearing in the record, as well as the relevant law firms appointed as curators)

should not be notified of the breach of personal data security. In this connection, the Digital Agency has stated that this is because the log files document that the accesses have not been used, which is why it is the agency's assessment that this is not a security breach that probably entails a high risk for the rights and freedoms of natural persons.

3. Reason for the Data Protection Authority's decision

On the basis of what was disclosed by the Danish Data Protection Agency, the Danish Data Protection Agency assumes that, due to human error, the Danish Data Protection Agency granted 26 curators access to the wrong companies' digital mailboxes.

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, cf. Article 32, of adequate security will normally mean that in systems with a large number of confidential information about a large number of users, higher requirements must be placed on the care of the data controller in ensuring that there is no unauthorized access to personal data, and that with access to data in such systems, greater requirements are placed on safeguarding against the possibility that a single human error could result in a major breach of personal data security.

The Danish Data Protection Authority is of the opinion that granting access to mailboxes belonging to third parties, also where a curator is given access to the estate's assets and digital mail, must be verified before the access is implemented. It will therefore normally be an expression of adequate security that, before access is opened, a check is made to ensure that it is the trustee - who has been appointed - who actually gets access.

Based on the above background, the Danish Data Protection Authority finds that the Digital Agency - by not having introduced measures to ensure that the lists were correct, and - according to the information - based the assurance solely on the fact that no human errors had previously occurred - has not taken appropriate organizational and technical measures to ensure a level of security that matches the risks involved in the agency'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 is a basis for expressing criticism that the

Digital Agency'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 response in a stricter direction, the Danish Data Protection Authority has emphasized that the Digital Agency has experienced similar errors before in the notifications on the Danish Data Protection Authority's cases with j.nr. 2020-442-10578 and 2020-442-9811, and that it is widely known that human errors occur, which is why safety cannot – alone – be based on a belief that humans do not make mistakes.

The Danish Data Protection Authority has noted that the Digital Agency has subsequently implemented a multi-eye principle on the lists of company mailboxes to which the agency gives access.

[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).