Serious criticism: Unintentional access to information about children

Date: 25-08-2022

Decision

Private companies

Serious criticism

Supervision / self-management case

Reported breach of personal data security

Access control

Treatment safety

Children

Unauthorized access

Unintentional disclosure

The Danish Data Protection Authority expresses serious criticism of KMD for not having tested a new functionality in a system sufficiently, which led to foster parents inadvertently gaining access to information about foster children in AULA.

Journal number: 2021-431-0126

Summary

The Danish Data Protection Authority has made a decision in a case where, based on reports of a breach of personal data security from a number of municipalities, the Danish Data Protection Authority initiated a case of its own initiative against the municipalities' data processor KMD.

The breach consisted of foster parents having had accidental access to information about foster children in AULA.

The reason for the breach was that a new functionality in a system that KMD used as a data processor had not been tested sufficiently, including how the functionality worked together with e.g. AULA.

On this basis, the Data Protection Authority found grounds for issuing serious criticism of KMD.

Decision

In the period from 19 January to 21 January 2021, the Norwegian Data Protection Authority received notifications about breaches of personal data security from six municipalities. It appeared from the reports that a system error in January 2021 at

the municipalities' data processor, KMD A/S (hereafter KMD), had led to the breach of personal data security, which had meant that foster parents had unauthorized access to AULA.

Against this background, the Danish Data Protection Authority initiated a case of its own accord against KMD on 1 March 2021.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that KMD'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

In the period from 19 January to 21 January 2021, the Danish Data Protection Authority received six notifications about breaches of personal data security from Skanderborg Municipality, Lemvig Municipality, Herning Municipality, Halsnæs Municipality, Haderslev Municipality and Tønder Municipality, respectively (Data Protection Authority's j.nr. 2021-442- 11376, 2021-442-11365, 2021-442-11340, 2021-442-11339, 2021-442-11373 and 2021-442-11363). The reviews related to the same security breach.

It appeared from the reports that there had been a transfer of information about foster parents to AULA from systems that KMD ran as a data processor for the municipalities, which meant that foster parents had had unauthorized access to information about, among other things, foster children in AULA.

Of the notifications of breaches of personal data security that the Danish Data Protection Authority received from the six municipalities above, as well as from the statements that the Danish Data Protection Authority received from other affected municipalities – Egedal Municipality, Læsø Municipality, Ringkøbing-Skjern Municipality, Tårnby Municipality, Samsø Municipality, Holstebro Municipality, Copenhagen Municipality, Horsens Municipality, Skanderborg Municipality, Billund Municipality, Struer Municipality and Lyngby-Taarbæk Municipality - it appears that information on at least 23 foster children has been affected by the breach. The information included contact details and social security numbers. In addition, the foster parents have had access to AULA, where other personal data may appear.

It also appears from the information in the case that the municipalities' data processor KOMBIT A/S (hereafter KOMBIT) was

also involved in the incident.

On 1 March 2021, the Danish Data Protection Authority requested KMD for an opinion for use in the processing of the case. The Danish Data Protection Authority also sent a number of additional questions to the case on 11 March 2021. KMD answered the Data Protection Authority's inquiries in a statement of 26 March 2021.

On 12 April 2021, the Norwegian Data Protection Authority asked KOMBIT for an opinion on the case. KOMBIT responded to the Danish Data Protection Authority's inquiry in a statement of 29 April 2021.

On 11 May 2021, the Danish Data Protection Authority asked the municipalities that were affected by the breach for an opinion for use in the processing of the case. In the period until 26 August 2021, the Norwegian Data Protection Authority received responses from all the municipalities.

2.1. KMD's remarks

It appears from KMD's statement of 26 March 2021 that Tønder Municipality approached KMD on 18 January 2021 to draw attention to the fact that there had been a transfer of information about foster parents from Institution I2 - which KMD operates as a data processor for the municipalities – for AULA, operated by KOMBIT. In this connection, KMD became aware of the breach and confirmed it the same day.

KMD has stated that the security breach involved several IT solutions that are part of the transfer of information about foster parents, including KMD Institution I2, the interface solution WS10 and the recipient system AULA at KOMBIT.

KMD has stated that the error was due to a new feature that KMD had to implement causing foster parents who should not have access to the AULA to inadvertently gain access to the AULA and information about foster children.

In this connection, KMD has stated that the cause of the breach could not be detected by KMD when testing the systems for which KMD was responsible, as the fault could only – according to KMD – be detected by testing the recipient system AULA. The tests carried out by KMD consisted of investigating whether the new function – where an active report on which data should and should not be transmitted – worked as intended. It was thus tested whether data was correctly forwarded after the active report, but not how the transmitted data was used in the recipient system AULA at KOMBIT.

KMD has stated that testing was done by going into the user interface, setting values and verifying that the values took effect correctly upon transmission. Since the test did not include how data was received in the receiving system, the test could not clarify how the transmitted data was used. In this connection, KMD has stated that if there was a test environment in the

recipient system, the possibility of the error could be reduced.

On January 18, 2021 – after the breach had been confirmed by KMD – KMD launched an analysis and correction of the erroneous transfers of information in the database. In addition, a new automatic transfer of information to AULA was completed without foster parent information. A termination test was also performed to verify that the change had resolved the issue, which was confirmed. The incident was then closed and notification of the breach was sent to the data controllers, corresponding to the 19 municipalities that had been affected by the incident.

On 11 March 2021, the Danish Data Protection Authority approached KMD with a question as to whether the incident is identical to an incident from November 2020 (registered with the following record numbers with the Danish Data Protection Authority: 2020-442-10386, 2020-442-10452, 2020-442-10445, 2020-442-10440, 2020-442-10419, 2020-442-10394, 2020-442-10396, 2020-442-10401, 2020-442-10410, 2020-442-10438). In a statement of 26 March 2021, KMD has stated that the previous breaches from November 2020 are not identical to the current incident. In this connection, KMD has stated that the breach in November 2020 concerned the solution KMD Institution I1 (and not I2).

KMD has stated that in connection with the breach from November 2020, personal data was transmitted from Pdata to KMD Institution I1, with which the information could be included in the regular data transmission package to STIL using the interface WS10. The error was due to a misinterpretation of the interface documentation from Pdata, and meant that protected information (name and address) was accessible to unauthorized persons. The security breach from November 2020 was also caused by human error, while the security breach from January 2021 – according to KMD – was caused by technical conditions.

The Danish Data Protection Authority did not express criticism in connection with the reports.

2.2. KOMBIT's remarks

It appears from KOMBIT's statement of 29 April 2021 that AULA gets all its data from STIL, and that all administration of content in AULA takes place in the municipalities' administration systems, such as KMD Institution I2, which continuously supplies data to STIL's basic school data through WS10 at STIL .

Every day at 01:00, AULA retrieves all updates from the past 24 hours for all users of AULA through WS17, which is the interface to which AULA subscribes. AULA thus does not receive data directly from KMD through WS10. Once the changes are downloaded, AULA updates all changed data with the updated data. No changes are made to this data in AULA. The

authority responsible for data is responsible for ensuring that data and updates thereof are correct, and therefore a recipient system such as AULA will assume that data is correct when it is received from the approved supplier. AULA thus does not receive data directly from KMD through WS10, but from STIL through WS17.

KOMBIT has stated that KOMBIT is a data processor in connection with AULA, and Netcompany A/S is a sub-data processor. Netcompany A/S helps to test changes on AULA's test systems if other suppliers request it. KOMBIT has also stated that it is possible to test changes on AULA's test systems if the municipality's suppliers request it. Similarly, it is possible to test data received from STIL through WS17 and processed in AULA, if the municipalities' suppliers also request it.

It is KOMBIT's opinion that the overall responsibility for the incident lies where the changes are initiated.

2.3. The municipalities' comments

By letter of 11 May 2021, the Data Protection Authority has addressed the 19 municipalities that have been affected by the incident with a view to obtaining opinions for use in the processing of the case. Several of the municipalities involved have jointly submitted a response to the Data Protection Authority's inquiry, as the municipalities consider a joint municipal follow-up on the issue to be expedient.

The municipalities have stated that they find it extremely critical that KMD has not complied with their obligation, cf. the data processing agreement, between the municipalities and KMD, to follow their own procedures for change management, with a view to ensuring that any change is properly authorised, tested and approved before implementation.

The municipalities have stated that, on the basis of the data processing evening, they have a justified expectation that KMD's internal test procedure and dialogue/test with KOMBIT/AULA will pick up serious errors before transition to production. The municipalities will sharpen this expectation towards KMD.

The municipalities have also stated that they will make a joint inquiry to KMD as a follow-up to the current incident. The inquiry will contain a tightening of compliance with the applicable data processing agreement. In this connection, KMD must explain how they will in future test changes to cut surfaces before commissioning/operation - including how this is ensured:

that the interface is checked end-to-end so that data is sent and received correctly

that KMD continuously updates the procedure for change management, so that new functions are properly tested before they are transferred to the production environment

that KMD initiates a dialogue with KOMBIT in connection with testing of changed cutting surfaces.

The municipalities will also recommend KOMBIT to once again make their collaboration partners, including KMD, aware of the testing opportunities available in the AULA environment.

3. Reason for the Data Protection Authority's decision

Based on the information in the case, the Danish Data Protection Authority assumes that it has been possible for KMD to carry out tests of the interaction of the new functionality with AULA, including by being able to carry out tests in AULA itself.

3.1. Article 32 of the Data Protection Regulation

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 for adequate security will normally mean that when a new functionality is developed for IT systems that must process personal data, the changes must be made according to agreed principles, where possible consequences of the change are considered and tests are planned, which can verify that security requirements are still met after the change has been implemented.

As far as IT systems are concerned, for which the data processor is not itself responsible, but where the data processor is responsible for significant input in the form of personal data, the Danish Data Protection Authority is of the opinion that the requirement for adequate security will normally mean that the data processor must create the necessary overview over own IT architecture and IT environment, including the systems which are integrated with other systems by delivering or receiving data, and where loss of integrity of personal data will entail a significant risk for the rights of the data subjects, and ensure a mapping of the integrations and associated dependencies.

As a result of the above, the data processor has a duty to report code changes in integrated systems to relevant data controllers and/or data processors for the integrated external systems before they go into production. These requirements must ensure that external data controllers and/or data processors are informed in a timely manner of the planned changes and can carry out appropriate tests of the integrity of personal data exchanged between the integrated systems.

Against this background, the Danish Data Protection Authority finds that KMD - by not having carried out appropriate tests of

the new function in KMD Institution I2 - has not taken appropriate organizational and technical measures to ensure a level of security that suits the risks involved in KMD's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has emphasized that the changes implemented by KMD should only have been tested on the basis of the data protection regulation's requirements for appropriate security measures. The Danish Data Protection Authority has further emphasized that various extracts of contracts/data processing agreements submitted by data controller municipalities imply that the data controllers could rightly expect that the IT solution was tested for the type of error that led to the breach of personal data security.

The Norwegian Data Protection Authority finds that the fact that the error was discovered by users in the municipality shortly after commissioning substantiates that the error could have been found in connection with a test.

The Danish Data Protection Authority has also emphasized that a change such as the one that has led to this breach is an intervention that should be carried out with extra attention to what consequences the change may have.

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

The Danish Data Protection Authority has considered it an aggravating circumstance that in November 2020 the Danish Data Protection Authority dealt with an incident concerning the same systems that supply data to AULA. The Danish Data Protection Authority is aware that the incident at that time is not identical to the current incident. The Danish Data Protection Authority has, however, attached importance to the fact that the incident at that time was also discovered by the users instead of by the data processor who made the changes in the IT solution, and that the problem of lack of testing should have been solved earlier.

The Danish Data Protection Authority has noted that the municipalities will make a joint inquiry to KMD as a follow-up to the current incident, and that the incident will contain a tightening of compliance with the applicable data processing agreement.

[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).