The Danish Data Protection Authority expresses serious criticism of Kombit's processing of personal data as a data processor for a number of municipalities

Date: 23-02-2022

Decision

Public authorities

Serious criticism

Reported breach of personal data security

Sensitive information

Unauthorized access

Treatment safety

The Danish Data Protection Authority has made a decision in a case where 30 municipalities had reported a breach of personal data security in Aula to the Danish Data Protection Authority

Journal number: 2020-442-6168

Summary

On 23 February 2022, the Danish Data Protection Authority made a decision in a case where 30 municipalities had reported a breach of personal data security to the Danish Data Protection Authority at the end of 2019 and the beginning of 2020.

The breach concerned that an error in Aula meant that from 24 November 2019 to 20 December 2019 it was possible for a user A to access another user B's secure files in Aula if user B was not logged out of the computer , and user A logged in with his own NemID. Secure files is an area in Aula with sensitive personal data that requires an additional login.

The error was due to a programming error at Netcompany in connection with the development of a change to the login solution in Aula.

For use in the case, the Data Protection Authority obtained a statement from Gentofte Municipality, which was one of the 30 municipalities that had experienced a security breach, as well as Kombit and Netcompany.

The Danish Data Protection Authority found that Kombit had not complied with the rules on processing security, as Kombit had not ensured that sufficient testing of Aula was carried out in connection with the change to the code in Aula.

The Danish Data Protection Authority emphasized that an error in the development of the solution meant that there was no

correct management of access rights in Aula.

The Danish Data Protection Authority also emphasized that Netcompany and Kombit could not agree on which tests could be expected to be carried out in connection with the development project, and that they could not agree on whether Netcompany acted as sub-data processor or not.

Against this background, the Danish Data Protection Authority issued serious criticism of Kombit.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Kombit's processing of personal data – as a data processor – 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 an error in Aula meant that if user A logged into Aula and left the computer without closing/logging off, after which user B accessed the computer where user A was logged in and user B accessed content, that required a "step up" in security level, user B would be asked to enter his NemID. Here, the system should only accept user A's NemID. If user B entered his own NemID, however, user B gained unauthorized access to user A's content.

It also appears from the case that the login to Aula that user A made was a one-factor login in the form of a UNI login. The subsequent login with NemID was a two-factor login that provided the necessary "step up" in authorization, which gave access to sensitive and confidential personal data in an area called "secure files".

The municipalities became aware of the breach following an inquiry from Kombit.

2.1. Gentofte Municipality's comments

Gentofte Municipality has stated that it is not possible to state how many people had the opportunity to obtain unauthorized access to personal data during the period in which the breach took place, since the exploitation of the error assumed that the user, contrary to the municipality's guidelines, had left his equipment to another user. In this connection, Gentofte Municipality has stated that approx. 1,500 user profiles for the municipality's employees who have potentially had the opportunity to access each other's secure files.

Gentofte Municipality has also stated that "secure files" are a special area of the Aula system, where there is increased

security to be able to access them in the form of a requirement for logging in via NemID, and that it was this extra security that, due to a programming error did not work as it should, as Aula mistakenly accepted any NemID, and not just the NemID that belonged to the user who had originally logged in - and who had not made sure to log out before handing the computer over to someone else user.

In addition, Gentofte Municipality has stated that what types of personal data are contained in "secure files" is to some extent up to the individual schools and Aulateams, as it is not possible to create such a precise application strategy that it is possible to centrally control which sensitive information must be in "secure files" - but the application strategy states that sensitive personal data must be in "secure files" and not elsewhere in Aula. It also appears from the application strategy that Aula is not a case management system. "Secure files" in Aula therefore primarily contain observations of children and classes, and not case processing, as this takes place in the municipality's ESDH system.

Gentofte Municipality has stated that a total of 7,684 students in the municipality are affected by the breach. However, each individual teacher will only have access to information on approx. 100-200 users.

Finally, Gentofte Municipality has stated that it is not the municipality's assessment that their users leave computers unlocked and that computers are automatically locked after a few minutes of inactivity. In addition, it will normally only be employees subject to confidentiality who may have used a shared computer.

2.2. Netcompany's remarks

Netcompany has stated that, in connection with the reported incident, a programming error had occurred during the development of a change to the login solution in Aula. It was a human error made by a developer at Netcompany. The error consisted of a programming error in the software's source code, which inadvertently disabled a so-called authentication test on one of Aula's login solutions. The authentication test is implemented on all Aula's login solutions and is an additional security measure that ensures that the user who is logged in is the same user as the one who tries to access the particularly sensitive areas of Aula. This is in order to protect users' personal data as much as possible.

Netcompany has also stated that despite Netcompany's extensive tests, which are carried out every time a new code is put into operation, the error was not discovered before the new code was implemented in Aula. Netcompany has also noted that the affected login solution had also previously been thoroughly tested, and that there was no reason to believe that the new source code would affect the login solution in question in connection with the implementation.

Netcompany has stated that the Aula project involves continuous further development, maintenance and operation of the system. It is therefore important to keep a sharp distinction between when Netcompany acts as sub-data processor and when Netcompany does not act as sub-data processor, as the latter i.a. is the case during the development and maintenance of Aula.

In addition, Netcompany has stated that the error – and part of the reason for the breach – occurred in the design/programming of Aula, and thus as part of the development of the solution. Since the development of software, such as Aula, does not constitute a data processing activity, Netcompany has stated that Netcompany has not acted as either data controller, data processor or sub-data processor in connection with the development of Aula and in connection with the resulting data breach.

In this connection, Netcompany has stated that the data breach could only occur in a case where another user failed to log out of his profile in violation of internal guidelines and normal user behaviour.

Netcompany has stated that a wide range of information in Aula can be accessed using one-factor login either via Uni-login or IdP-login (for employees). This was in accordance with the wishes of the municipalities and Kombit that it should be easy to access the Aula, as there was a concern that users would not use the Aula if the access control was too difficult. Sensitive and confidential information can only be accessed with two-factor login. Aula was originally built in such a way that the areas that contained sensitive information, e.g. "secure files" or "sensitive messages", required an additional login, in the form of NemID. In both the Uni and IdP login solutions, users initially logged into Aula with username and password (one-factor), after which they had to use their NemID (two-factor) to log in again to access sensitive areas of Aula, as there was a so-called "step-up" in security.

Netcompany has also stated that at one point the municipalities and Kombit wanted to implement a solution in the IdP login solution, where it became possible to carry out two-factor login ("step-up") using a local IdP instead of NemID , so that you logged in with a local idP (one-factor) and "stepped up" with a local idP (two-factor). In accordance with the processes in an IT development contract, a change request ("ÆA43 – step-up with Local IdP") was therefore prepared on 8 October 2018. The change went live with release 1.1.5 on November 24, 2019.

When release 1.1.5 was commissioned on 24 November 2019, an error occurred in Aula's handling of the UNI login solution. This happened because a code was introduced in release 1.1.5, which inadvertently disabled the automatic authentication test

in the UNI login solution, so that it was no longer ensured that the user logged into Aula was the same user who the one who tried to "step-up" when approaching the sensitive areas in the Aula. It was a human error in the programming made by a developer at Netcompany. Netcompany received notification of the error at 8.30 on 20 December 2019 and had resolved the error after four hours.

Netcompany has claimed that when the specific situation, such as the one at hand, can arise - where user A does not log out of his Aula profile and leaves his computer unlocked, after which user B can access user A's profile and from there try to "step-up" with its own NemID - then this is because neither Netcompany, F-secure (which carried out an additional penetration test in connection with release 1.1.5), Kombit or the municipalities had reason to believe that the new programming code, which only concerned IdP -login solution, could affect the UNI login solution, and that there was therefore a need to test the UNI login solution further. The UNI login solution had previously been thoroughly tested without any errors being found in the solution, nor was there any reason to believe that errors would occur in the solution when implementing release 1.1.5.

Finally, Netcompany has claimed that it was approved by Kombit, that it was only the IdP login solution that was tested in connection with the release, and that all test routines at Aula in addition and throughout the project have been assessed and approved in accordance with the processes under a development agreement.

2.3. Kombit's remarks

Initially, Kombit stated that, as a total supplier of the Aula solution, Netcompany processes personal data. This processing takes place exclusively on behalf of the municipalities for the purposes specified by the municipalities, as Kombit has imposed on Netcompany the same data protection obligations that Kombit has been imposed on by the municipalities. It is therefore Kombit's assessment that this is a sub-data processor construction in the relationship between Kombit and Netcompany.

In Kombit's view, the fact that it is a sub-data processor structure between Kombit and Netcompany is not changed by the fact that Netcompany, as part of the overall services to be delivered under the contract, solves tasks that do not directly entail the processing of personal data. Kombit therefore does not agree with Netcompany that a distinction must be made between when Netcompany acts as sub-data processor and when Netcompany does not act as sub-data processor.

Kombit has stated that in the change request ÆA 43 – Step-up with local IdP, Kombit wanted a new functionality in Aula. Kombit did not make demands on how Netcompany should change Aula's code in order to achieve the new functionality, as Kombit's knowledge of the solution was not at such a level of detail that it would be possible for Kombit to write a requirements

specification for the change on the code level.

In this connection, Kombit has stated that Netcompany in ÆA 43 pt. 3.5 has stated:

"Development and execution of test cases related to this change request will be carried out in accordance with the releases in which the various parts will be delivered. Functional testing and regression testing will be performed focused around the areas where functional changes have been made".

In Kombit's view, it is Netcompany that is closest to determining the scope for the functional test and regression test, as it is Netcompany that has knowledge of where changes have occurred in the code caused by ÆA 43. In ÆA 43, Netcompany has assessed, that since it is an extension of the login and local IdP handling – a complex model that requires a special setup for testing, the estimation profile 'Extra test' is used. Kombit has stated that it appears from ÆA 43 that 118 hours are set aside for "testing" and 31 hours for "additional testing - API versioning". When approving the change request, Kombit was therefore of the view that Netcompany had tested all parts of the login solutions where functional changes had been made. In this connection, Kombit has stated that Kombit had not specifically approved that it was only the IdP solution that was tested.

Kombit has stated that Netcompany should be the closest to ensuring that sufficient tests are carried out when Netcompany makes changes to the solution, as Netcompany is the closest to assessing how the changes implemented by their developers will affect other parts of Aula- the solution.

3. Reason for the Data Protection Authority's decision

Based on the information provided to the case, the Danish Data Protection Authority assumes that from 24 November 2019 to 20 December 2019 it was possible for a user to access another user's secure files in Aula, if that person was not logged out of the computer.

On this basis, the Danish Data Protection Authority assumes that there has been unauthorized access to personal data, which is why the Danish Data Protection Authority finds that there has been a breach of personal data security, cf. Article 4, No. 12 of the Data Protection Regulation.

The Danish Data Protection Authority also assumes that the error occurred due to a programming error in release 1.1.5, which concerned the IdP login solution, which put user authentication in connection with "step-up" out of play on the UNI login solution, and that there was about a human error.

It follows from the data protection regulation article 32, subsection 1, that the data controller and the data processor must take

appropriate technical and organizational measures to ensure a level of security suitable for the risks involved in the data controller's processing of personal data.

Thus, the data controller and the data processor have 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 for adequate security will normally imply that all probable error scenarios should be tested in connection with the development and modification of software where personal data is processed.

The Danish Data Protection Authority finds that Kombit – by not having ensured that sufficient testing was carried out of Aula, including in the UNI login solution, in connection with the change of the code in Aula – has not taken appropriate organizational and technical measures to ensure a level of security, that matches the risks involved in Kombit's processing of personal data, cf. the data protection regulation's article 32, subsection 1.

The Danish Data Protection Authority has emphasized that an error in the development of the solution meant that there was no correct management of access rights in Aula.

The Danish Data Protection Authority has also emphasized that Netcompany and Kombit could not agree on which tests could be expected to be carried out in connection with the development project, and that the same parties do not appear to agree on whether Netcompany acted as sub-data processor or not, which can lead to to deficiencies in treatment safety. It is the opinion of the Data Protection Authority that the instructions from the data controller must state clearly how such a disagreement is to be handled. Furthermore, the Danish Data Protection Authority is of the opinion that no sub-data processor can make decisions on their own about concrete matters regarding what security is required when the changes to be carried out actually affect processing that is solely under the responsibility and instructions of the data controller, and this cannot be unambiguously derived from the data controller's instructions to the data processor.

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

In relation to the choice of sanction, the Danish Data Protection Authority has emphasized the following as aggravating

circumstances:

That the extent of the breach could not be uncovered, but in Gentofte Municipality alone there were approx. 1,500 people whose access could be misused under the right circumstances.

That the affected information may be information worthy of protection about many minors. In Gentofte Municipality alone, they could affect several thousands, without it being possible to reveal more.

That there does not seem to be clarity about the division of responsibilities between Kombit and Netcompany.

As extenuating circumstances, the Danish Data Protection Authority has emphasized:

That there is limited access for people who normally have access to the same type of information.

That the error could only be exploited in combination with the fact that a user did not protect his login.

[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).