Region North Jutland receives criticism for a lack of security around self-service solutions

Date: 08-11-2021

Decision

Public authorities

Criticism

Reported breach of personal data security

Unauthorized access

Treatment safety

Data processor

Notification of data subjects in the event of a breach of personal data security

The Danish Data Protection Authority has made a decision in a case where Region Nordjylland has reported a breach of personal data security regarding a vulnerability in a self-service solution.

Journal Number: 2021-442-12924.

The Danish Data Protection Authority hereby returns to the case where the North Jutland Region reported a breach of personal data security to the Danish Data Protection Authority on 8 May 2021. An internal reference number is stated in the notification: 2021-017514. The report has the following reference number: 2ca746503d826e268cbc6d6f23c1543aa7b67c1d.

Summary

From May 2018 to April 2021, it has been possible - via an IT solution - to access other people's personal data and cancel bookings, e.g. appointments at a hospital. It was a well-known type of vulnerability that concerns the lack of control of user access. Misuse of the solution required the user to be logged in with NemID, but the error meant that access to bookings and letters was not limited to the current user's own bookings/letters.

The Danish Data Protection Authority has expressed criticism that Region Nordjylland had not met the requirement for appropriate security measures, because the region had not set sufficient security requirements in its agreements with the company that developed the solution.

The Danish Data Protection Authority emphasized that the personal data of potentially half a million registrants could have

been accessed by unauthorized persons, that the information included health information and other information worthy of protection, that both the confidentiality and availability of the personal data could be affected, and that the breach had been ongoing for approx. three years.

Furthermore, the Danish Data Protection Authority emphasized that the breach of personal data security was due to a known type of vulnerability, and thus something that should have been dealt with already during the development and testing of the IT solution.

In a mediating direction, the Danish Data Protection Authority has emphasized, among other things, that abuse of the vulnerability should take place behind a login with NemID, which – although it could not prevent the possibility of abuse – would nevertheless give users the impression that they might be exposed if they exploited the vulnerability and that this could possibly deter them from doing so.

1. Decision

After a review of the case, the Data Protection Authority finds that there is a basis for criticizing the fact that Region North Jutland'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 Regions Nordjylland's data processor discovered an error in the IT solution "MineAftaler", which made it possible during login with NemID to change a number in a REST service URL and thereby gain access to other citizens' personal data.

It appears from the case that the breach of personal data security has existed from 30 May 2018 in the IT solution "SelvBooking" (i.e. from the time the IT solution was put into use). The IT solution was subsequently further developed into the "MineAftaler" solution, which was put into use on 10 February 2021. The breach existed in "MineAftaler" until it was discovered on 29 April 2021 by the company that is the data processor in relation to the processing of personal data in "MineAftaler", and which is also the developer and supplier of "MineAftaler". "MineAftaler" is included as a module in the booking system "BookPlan", which Region Nordjylland receives from the data processor.

Region Nordjylland has informed the case that after logging in with NemID, you could change a number in a URL and thereby

with a certain probability access other people's bookings. This is elaborated in two rounds:

It is not a direct URL in the browser that you can correct. It is a REST service that the web application uses under the hood.

The URL of the REST service is: https:<host>:<port>/selvbooking/rest/breve/<letter ID>.

It must be emphasized that it was not possible to look up a certain person's received correspondence from Region Nordjylland without knowing the specific URL address behind it. If there is a change in the underlying URL address, an arbitrary letter would be displayed instead, if the change happened to match this.

...

"The URL, which the user had to correct, had to be found in the browser's Developer Console, so that you can see what network traffic there is from the application to the backend. Then find the REST call in question and change the parameters (<letter ID>), guessing a new available <letter ID> (there are a lot of gaps in the sequence, so it wasn't all consecutive letter IDs' are that could be found)."

It also appears from the case that this is a vulnerability described at https://owasp.org/www-project-top-ten/, specifically the vulnerability A5:2017-Broken Access Control. To correct the error, the data processor implemented the correct use of Access Control, after which the authenticated user can only post on data that belongs to the user himself.

Region Nordjylland has stated that there is a limited amount of users of "MineAftaler", but everyone with a NemID who has been logged in during the period 30 May 2018 to 29 April 2021 has had the opportunity to exploit the vulnerability. The vulnerability gave access to all letters printed to patients before 30 April 2021, which per 30 April 2021 includes 498,599 patients. This includes information about name, private address, social security number and health information. The latter is, as a general rule, a clinical department, form of consultation, including purpose of consultation, possibly reply letters, which state what the result of an examination is - however not if it is a question of confirmed illnesses of a significant nature.

The region has not been able to confirm or deny whether there were secret addresses among the affected personal data.

The vulnerability made it possible to delete other people's letters and bookings. However, Region North Jutland estimates that this would have been discovered in most cases due to other communication between patients and hospitals.

Examining the logs has shown that no abuse has occurred in the last 180 days leading up to the discovery of the breach. In the period starting from June 2020, only "mass harvesting" of letters could be investigated, of which there were no indications. For the rest of the period when the breach was ongoing, it could not be clarified whether there were indications of abuse.

Region North Jutland has explained the period for storing the log with a reference to the security order:

RN has, in accordance with the previously applicable security order, which the Danish Data Protection Authority has previously stated must continue to apply as a guide for security in the public sector's safeguarding of the processing of personal data in the public sector, has chosen to set the audit log period at 180 days.

As documentation for measures carried out before the breach was detected, Region North Jutland has forwarded an IT contract and data processing agreement. The region has also specified a GDPR audit of the data processor carried out in January 2021 (i.e. immediately prior to the commissioning of MineAftaler) as a measure.

In relation to the IT contract (Delivery Agreement of 8 April 2013), the Danish Data Protection Authority has read parts of it. Point 5 mentions Factory Acceptance Test (FAT), User Acceptance Test (UAT), load test and function test (Smoke test) as well as Installation test, Takeover test (OP) and operation test, without the precise content of these being described in more detail in the IT contract. Point 7 describes, among other things, that the purpose of the OP is to ascertain whether the delivered functionality and documentation in the partial delivery in question meets the requirements of the agreement. In relation to other "tests", these are linked to some "acceptance criteria", which, however, are not further described in the IT contract.

The submitted data processing agreement was entered into in September 2013 and updated on 20 January 2020. The original agreement mentions that it concerns the supply, operation and maintenance of the IT system for clinical booking. The updated data processing agreement concerns the processing of personal data for the purpose of fulfilling the "Clinical Booking Delivery Agreement", and it mentions, among other things, that Annex 1 (Data processing instructions) specifies minimum requirements for the necessary technical and organizational security measures. These requirements include, among other things, following:

4.2.3 The data processor must document the identified risks and how the risk has been reduced to an acceptable level.

The above obligation implies that the data processor must carry out a risk assessment and then implement measures to address identified risks. This may include, depending on what is relevant, the following measures:

Pseudonymisation and encryption of personal data

Ability to ensure ongoing confidentiality, integrity, availability and robustness of processing systems and services

Ability to promptly restore the availability of and access to personal data in the event of a physical or technical incident

A procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing safety.

As documentation for tests that are relevant to the breach, and carried out before MineAftaler/SelvBooking was put into use, Region Nordjylland has forwarded the data processor's test cases in the "Testcases-MineAftaler-Copyright" spreadsheet.
The GDPR audit, which is also described as a measure, was completed on 14 January 2021, and showed, among other things, that in relation to "Processing security and Privacy-by-Design and Privacy-by-Default" a compliance level of 73% was assessed, with 100% being the best. In the audit, the assessment is followed by a recommendation with the following wording: "The data controller should ensure that the data processor's compliance score within the theme is raised, as the compliance score – based on the data processor's answers to the questions included in the DPA Service – is assessed as a means." The Norwegian Data Protection Authority has not received information on whether the recommendation has been followed.
It also appears in the case that the notification of the breach took place approx. 9 days after the breach was discovered.
Region North Jutland has justified the delay as follows:
The vulnerability was closed immediately on Friday, April 29, 2021 in the afternoon. The solution was removed immediately and only reopened when the hole was closed. The delayed notification is due to further investigations into the possible extent of the breach at the supplier with a view to RN assessing whether there was compromised data during the breach period.
RN accepted that the supplier completed a preliminary investigation of the course of events to assess whether a breach had occurred which posed a risk to the rights of the data subjects, or whether this could be ruled out, after which notification to the data protection authority was not mandatory, cf. Article 33 of the data protection regulation , PCS. 1. Since RN's knowledge of the breach was dependent on the supplier's investigation, this could not be reported within 72 hours, but was dependent on the supplier's preliminary investigation, which was given orally on 8 May, after which notification took place, as it could not be done with complete certainty it is excluded that there had not been a breach of personal data security. The written preliminary investigation was received on 12 May 2021.
In Region Nordjylland's documentation of the breach, cf. the data protection regulation, article 33, subsection 5, it is stated as an explanation why the data subject will not be notified of the breach, as well as the consequences of the breach:
Orientation to the registered? No. Due to the technical analysis, the probability is assessed as very low and the consequences are not assessed to have physical or financial consequences for the patients.
What are the consequences of the breach for the persons concerned? Probably none, as the information can only be accessed through a hacker attack and there are no indications of this. In addition, a maximum of letters can be changed or

deleted, which has not happened during the last 180 days.

3. Reason for the Data Protection Authority's decision

The Danish Data Protection Authority assumes, on the basis of what the Region of North Jutland has provided, that it has been possible to establish unauthorized access to personal data and to delete other people's letters and bookings

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.

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 cf. Article 32 for adequate security will normally entail that 1) in systems with a high number of confidential, including sensitive, information about a high number of people, stricter requirements must be placed on the care of the data controller when securing that there is no unauthorized access to personal data, and that 2) all probable error scenarios should be tested in connection with the development of new software to be used for processing personal data.

Based on the above, the Danish Data Protection Authority finds that Region Nordjylland – by failing to set sufficient requirements for the development and testing of new software – has not taken appropriate organizational and technical measures to ensure a level of security that is suitable for the risks involved in the region's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has emphasized that agreements had been concluded which concerned this particular IT solution and the processing of personal data therein, but that these agreements lacked a focus on data protection in the development and testing of the IT solution. The IT contract – which, among other things, is listed as part of the measures that were carried out before the breach was detected - does not make clear requirements for tests that have a security focus.

Certain test criteria are not detailed in the contract, and tests labeled as "User Acceptance Test" are typically not designed to reveal errors of the type encountered here, which can be misused. The Danish Data Protection Authority finds that the IT contract in particular, which is very specific about development and testing of the IT solution, should have contained clear requirements with a focus on security in development and testing.

In connection with the above, the tests - which Region Nordjylland has sent as documentation for tests that are relevant to the breach, and which were carried out prior to the commissioning of SelvBooking/MineAftaler - appear as function tests/user tests. They thus appear as tests with a primary focus on intended functionality and thus not vulnerability tests, penetration tests and similar tests with a focus on security - i.e. tests which primarily focus on unintended functionality that may can be abused.

After a review of the case, the Danish Data Protection Authority hereby finds that there is a basis for expressing criticism that Region North Jutland'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 to react in a stricter direction, the Danish Data Protection Authority emphasized that the personal data of potentially half a million registered persons could have been accessed by unauthorized persons, that the information included health information and other information worthy of protection, that both the confidentiality and availability of the personal data could be affected, and that the breach was ongoing in approx. 3 years. Furthermore, the Danish Data Protection Authority emphasized that the breach of personal data security was due to a known type of vulnerability, and thus something that should have been dealt with already during the development and testing of the IT solution.

The fact that a <letter ID> had to be specified and that there were "many gaps in the sequence, so not all consecutive letter IDs could be found", does not immediately appear to change anything in relation to the seriousness of the breach, given that the data controller has not disclosed any restrictions on the possibility of trying all possible values of <letter ID>.

The fact that a URL had to be changed, which could be found via the browser's Developer Console, immediately means that exploiting the vulnerability requires more technical knowledge than if the URL in the browser's address field had to be changed. However, the Danish Data Protection Authority considers that this does not make a big difference in relation to the risks the breach has posed. Malicious persons who have the intention and will to abuse a web application will usually also have an understanding of how web applications are developed/function, and thus how this type of vulnerability can be exploited.

When choosing a mediating response, the Danish Data Protection Authority emphasized that abuse of the vulnerability should take place behind a login with NemID, which - although it could not prevent the possibility of abuse - would nevertheless give users the impression that they might be exposed , if they exploited the vulnerability and that this could potentially deter them from doing so. The Danish Data Protection Authority has also emphasized that Region Nordjylland had a GDPR audit carried out prior to the commissioning of MineAftaler, even though this described the level of processing security, privacy by design/default as "medium".

The Data Protection Authority finds that the measure "GDPR audit" has less value, given the medium level, and the fact that the audit was carried out immediately before "MineAftaler" was put into use, and thus a long time after the original error-ridden solution "SelvBooking" was developed.

3.2. Article 33 of the Data Protection Regulation

It follows from the regulation's article 33, subsection 1, that in the event of a breach of personal data security, the data controller must report the breach to the Danish Data Protection Authority without undue delay, and if possible within 72 hours, unless it is unlikely that the breach of personal data security involves a risk to the rights or freedoms of natural persons.

Regions Nordjylland's justification for not reporting the breach earlier was that the data processor was given time to assess whether there was compromised data during the period in which the breach occurred (30 May 2018 to 29 April 2021).

The Danish Data Protection Authority assumes - in accordance with what the Region stated - that the solution was taken down on 29 April 2021, and it is stated on that occasion that the "hole" has been closed. Overall, it is therefore the Danish Data Protection Authority's assessment that both the data processor and the data controller - at the latest at this point - were aware that there had been a possibility of unauthorized access to personal data due to a vulnerability in "MineAftaler".

The Norwegian Data Protection Authority also assumes that the data controller awaited the results of an investigation into whether this vulnerability had been used by someone to gain unauthorized access.

The Danish Data Protection Authority is of the opinion that, in cases where there has been unauthorized access to personal data, and it cannot be objectively proven within 72 hours from the finding thereof, that such access has not been used, and that, cf. Article 33, therefore cannot is established, "... that it is unlikely that the breach of personal data security entails a risk...", notification must be made to the supervisory authority.

Completion of the investigation into an incident that is defined by Article 4, No. 12, cannot therefore justify exceeding the 72

hours.

The Danish Data Protection Authority therefore finds that the notification should have been made earlier than 8 May 2021, but the Danish Data Protection Authority has also noted that the delay was limited

3.3. Article 34 of the Data Protection Regulation

It follows from the regulation's article 34, subsection 1, that when a breach of personal data security is likely to entail a high risk for the rights and freedoms of natural persons, the data controller shall notify the data subject without undue delay of the breach of personal data security.

Region North Jutland has in their internal registration of breaches, cf. the data protection regulation, article 33, subsection 5, justified opting out of notification with a low probability, although without it being readable as to this probability ("Due to the technical investigation, the probability is assessed as very low..."). The assessment of the consequences of the breach is "probably none", but the wording is unclear ("the consequences are not assessed to have physical or financial consequences for the patients") - however, it seems to be justified that access to the information would require a "hacker attack and there are no indications of this".

If, in a specific situation, you do not have sufficient log data to confirm or deny that an access has been misused, this must be included in the assessment of risks for the data subject's rights, and thus in the assessment of whether the data subject must be notified of the breach .

The Danish Data Protection Authority must also note that Article 33, subsection 5 requires documentation of all breaches of personal data security, and this requires the quality of the internal registration. Region North Jutland's current registration does not give a clear impression of the considerations behind not notifying the affected registered parties.

The Danish Data Protection Authority assumes that the assessment of probabilities and consequences (and thus the risk for the affected data subjects) is based on the log data that only covers part of the period of the breach, which in the Danish Data Protection Authority's opinion is not sufficient to assess the risk as being low . When there is a lack of documentation as to whether a vulnerability has been abused, it implies a wide range in the possible consequences from "no consequence" to the worst imaginable in relation to the amount of personal data in particular, what the information can be misused for, and what the deletion of a letter or a booking could involve (if it is not discovered due to other communication between the citizen and the region).

On the basis of the overall information that the Data Protection Authority has received regarding the nature of the breach, the Data Protection Authority does not, on the present basis, find reason to override the region's choice to withhold notification.

However, the Danish Data Protection Authority recommends Region North Jutland to improve the quality of internal registration - and possibly the assessment – of a breach of personal data security.

In relation to Region Nordjylland's audit log, the Danish Data Protection Authority must note that when determining an appropriate logging period and content of the log, the region must take into account the purpose of the log and how it is used. If, for example, a data controller decides to make random samples in a log, then the log must be saved for the period that you want the random samples to cover (e.g. the last 3 months back in time). If a log is expected to be able to show abuse of user accesses – accesses that by mistake have not been terminated upon resignation – then the log must cover the maximum period that can elapse before such non-terminations are detected and corrected, so that the log can show all potential abuse during the period when access should have been discontinued. Another purpose can be investigations of hacker attacks, where the data controller chooses to follow the Center for Cyber Security's recommendations on storage periods for logs.

3.4. Summary

On the basis of the above, the Data Protection Authority finds that there is a basis for criticizing the fact that Region North Jutland's processing of personal data has not taken place in accordance with the rules in the data protection regulation[2] article 32, subsection 1.

4. Concluding remarks

The Danish Data Protection Authority notes that the Danish Data Protection Authority's decision cannot be appealed to another administrative authority, cf. Section 30 of the Data Protection Act.

However, the Data Protection Authority's decision can be appealed to the courts, cf. § 63 of the Basic Law.

For the sake of order, the Norwegian Data Protection Authority should note that the Norwegian Data Protection Authority expects to publish news about the decision and a copy of it on the Norwegian Data Protection Authority's website in one week.

The Danish Data Protection Authority hereby considers the case closed and will not take any further action in the matter.

[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).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to 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).