Serious criticism of the Danish Health Data Agency for unintended changes in the Common Medical Card

Date: 22-06-2022

Decision

Public authorities

Serious criticism

Reported breach of personal data security

Treatment safety

Notification of breach of personal data security

The Danish Data Protection Authority expresses serious criticism of the Health Data Agency for not meeting the requirement for adequate security. It was an aggravating circumstance in the supervisory authority's decision that the Danish Health Data Agency had previously made similar mistakes.

Journal number: 2021-442-14071

Summary

On the basis of a reported breach of personal data security, the Danish Data Protection Authority is now expressing serious criticism of the Danish Health Data Agency.

The breach occurred when a code change in the Health Platform (SP), where the Capital Region is the data controller, led to unintended changes in the Common Medical Card (FMK), where the Danish Health Data Agency is the data controller. The error meant that the removal of the dosage end date for 267 people on the Common Medicine Card did not make it through to the Health Platform.

As data controller for FMK, the Danish Health Data Agency has an obligation to take appropriate technical and organizational measures to ensure a level of security that suits the risks involved in the agency's processing of personal data in FMK.

This obligation implies that, as a starting point, the Danish Health Data Agency should test all probable error scenarios in connection with the development and change of software in FMK. In cases where a third party such as the Capital Region can make changes, the Danish Health Data Agency, as the data controller for FMK, is also responsible for these changes being tested.

This has not happened in this case, and thus, in the opinion of the Danish Data Protection Agency, the Danish Health and

Safety Authority has not met the requirement for adequate security.

In February this year, the supervisory authority ruled on a similar case, where a code change in SP led to unintended changes in FMK. In that case, it was the authority's assessment that the Capital Region, as the data controller for SP, was responsible for the security breaches.

In cases where several actors exchange data in a service-based architecture, the Danish Data Protection Authority often sees consequences in other systems than where the change has taken place.

Each data controller must establish the necessary guidelines and procedures for its own systems for how changes in source systems for which others are data controllers must be able to have impact. In particular, there must be procedures for service windows, change management, design requirements, testing of functionality and data integrity.

In relation to the previously decided cases, the Danish Data Protection Authority has found it essential to establish that a lack of robustness and a lack of integrity tests in FMK are also an expression of a lack of level of security.

In this decision, the Danish Data Protection Authority has also mentioned a number of initiatives that all data controllers in the service architecture must consider implementing. The frequency of errors in the chosen architecture is far too high in relation to the risk to the citizens whose information is processed. And these errors can only be rectified if all data controllers in the data chain actively collaborate on the necessary robustness and overall security of the entire solution.

The Danish Health Data Agency also exceeded the deadline of 72 hours for reporting a security breach – the agency became aware of the breach on 9 August 2021, but only reported it to the Danish Data Protection Authority on 13 August 2021.

Against this background, the Norwegian Data Protection Authority found grounds for expressing serious criticism.

Decision

The Danish Data Protection Authority hereby returns to the matter where the Danish Health and Data Protection Agency reported a breach of personal data security to the Danish Data Protection Authority on 13 August 2021. The report has the following reference number:

1eccb61d9b5ce4af09fd076d68784708b860ba53.

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 Health and Data Protection 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 and Article 33, subsection 1.

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

2. Case presentation

On 13 August 2021, the Danish Health Data Protection Agency reported a breach of personal data security to the Norwegian Data Protection Authority.

It appears from the notification and the subsequent follow-ups that, in connection with an update of the Health Platform on 17 March 2021, a code error occurred which resulted in the removal of end dates (treatment and dosage end date) on the Common Medicine Card (hereafter FMK) did not pass through to the Health Platform regarding the dosing end date for 267 affected individuals.

It also appears from the notification that on 9 August 2021, the Capital Region informed the Danish Health Data Agency by telephone about the breach. The Danish Health Data Agency is not aware of when the Capital Region discovered the error.

In addition, it appears from the notification that the Capital Region stated that the code error is expected to be corrected on 18 August 2021.

The Danish Health Data Agency has stated that the agency is the data controller for FMK, and including responsible for the integrity of data in FMK.

In this connection, the Danish Health Data Agency has stated that it is the individual users, in this case the Capital Region as data controller for the Health Platform, who are obliged to ensure that their system registers and communicates correctly with FMK.

The Danish Health Data Agency has stated that although the agency carries out quality control of FMK in the form of investigating cases of error and continuous quality assurance in the form of consumption control, the error would not have been discovered in this type of control.

The Danish Health Data Agency will therefore meet with the Capital Region and discuss whether they can jointly make improvements so that these mistakes do not happen again.

On 27 September 2021, at the FMK steering group meeting, the Capital Region informed the Danish Health Data Agency that a warning would be made in the Health Platform, which would address the error. The Danish Health Data Agency accepted the handling, and was later informed that the warning has been put into operation.

In addition, the Danish Health Data Agency has stated that in FMK, among other things, is a high degree of automated testing, a comprehensive test environment that the parties in the healthcare system can use. In addition, FMK has a man-year for release and test coordination. The Danish Health Data Agency also facilitates the use of systems that use FMK, meeting 1-2 times a year for a period of 1-2 days, where the focus is exclusively on testing.

In conclusion, the Danish Health Data Agency has stated that since the employee who reported the incident to the Danish Data Protection Authority is no longer in the organisation, the agency cannot explain in more detail why the breach was only reported on 13 August 2021.

3. Reason for the Data Protection Authority's decision

The Danish Data Protection Authority assumes, on the basis of what was disclosed by the Danish Health Data Agency, that in connection with an update in the Health Platform on 17 March 2021, a code error occurred, which meant that a removal of treatment and dosage end dates on FMK did not make it through to the Health Platform.

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 imply that all probable error scenarios should be tested in connection with the development and modification of software where personal data is processed. In cases where third parties can make changes, the data controller of the application and data therein is also responsible for testing changes made by others. It is the opinion of the Danish Data Protection Authority that there must be clearly agreed control mechanisms in place between all actors in a service-based architecture, control mechanisms that ensure that the data controllers for their processed personal data are in control and can ensure that misunderstandings in data formats or service structure do not result in that the integrity of the data is lost or corrupted. This can e.g. is done by organizational measures such as holistically updated system documentation, well-defined change management and related processes, fixed service windows for all actors in the entire data chain and subsequent testing, but

also technical measures such as signed and versioned services, integrity control of data, signing of data, built-in error checks in services are possible solutions to avoid errors.

The Danish Data Protection Authority finds, on the above background, that the Health Data Agency - by not having ensured that sufficient measures were taken, e.g. as a minimum test for integrity errors in FMK – has not taken appropriate organizational and technical measures to ensure a level of security that matches the risks involved in the Danish Health and Safety Authority's processing of personal data, cf. the data protection regulation's article 32, subsection 1.

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 entails a risk to the rights or freedoms of natural persons.

The Danish Data Protection Authority finds that the Danish Health and Data Protection Agency's processing of personal data – by reporting the breach too late – has not been done in accordance with the data protection regulation's article 33, subsection 1.

In this connection, the Danish Data Protection Authority has emphasized that the Danish Health Data Agency became aware of the breach on 9 August 2021, and that the agency first reported the breach on 13 August 2021.

3.3. Summary

On the basis of the above, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that the Danish Health and Data Protection Agency's processing of personal data has not taken place in accordance with the rules in the data protection regulation[2] article 32, subsection 1 and Article 33, subsection 1.

When choosing a more stringent response, the Danish Data Protection Agency has emphasized that the Danish Health and Data Protection Agency has experienced similar errors before in the Danish Data Protection Agency's cases with j.nr. 2020-442-8862 and 2021-442-13762.

[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 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).