Serious criticism, injunction and warning to the Capital Region after two security breaches

Date: 18-02-2022

Decision

Public authorities

Serious criticism

Injunction

Warning

Reported breach of personal data security

Basic principles

Sensitive information

Treatment safety

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

The Danish Data Protection Authority's decision comes on the basis of two security breaches, which were notified by the Danish Health Data Agency in August 2020 and July 2021. In both breaches, a data exchange service from the health platform - for which the Capital Region was responsible for data - was involved.

Journal Number: 2020-442-8862

Summary

The Danish Data Protection Authority has expressed serious criticism and issued an order and a warning to the Capital Region. The decision comes on the basis of two security breaches, which were notified by the Danish Health Data Agency in August 2020 and July 2021. In both breaches, a data exchange service from the health platform – for which the Capital Region was responsible for data – was involved.

In August 2020, the security breach affected 4,223 drug prescriptions for 2,310 patients, and in July 2021, the security breach affected 1,311 drug prescriptions distributed among 1,149 patients from the Capital Region and Zealand Region.

Code changes in one system caused unintended changes in another

Both security breaches occurred when code changes in the Health Platform (SP), where the Capital Region is the data controller, led to unintended changes in the Common Medicine Card (FMK), where the Danish Health Data Agency is the data

controller. The security breaches occurred on the basis that the integrations between FMK and SP enable an update in SP to affect the integrity of the display of information in FMK.

After reviewing both reported breaches, the Danish Data Protection Authority has issued serious criticism of the Capital Region for:

not having qualified relevant test scenarios in order to better identify dependencies to other IT systems,

not having completed necessary tests before the changes were put into production,

not having informed the Danish Health Data Agency about the security breaches when the incidents were detected,

It has also been an aggravating circumstance in the Danish Data Protection Authority's decision that the Capital Region did not sufficiently rectify the security after the first security breach in August 2020, and that a similar breach therefore repeated itself in July 2021.

The Danish Data Protection Authority has issued an order for the Capital Region to prepare and introduce a process that ensures that no changes to SP's functionality or data base are implemented and put into operation before it is ensured that no known integrations with other systems create incorrect information in these. The order thus covers not only integrations with FMK, but all IT systems that are integrated with SP. Including IT systems that have other data controllers.

The Danish Data Protection Authority has also issued a warning to the Capital Region that it is likely to be in breach of the data protection regulation to implement system changes in SP, where data integration with other systems occurs, without carrying out data integrity tests.

Detailed mapping and a better overview of data responsibility

In relation to the Danish Health Data Agency, the Danish Data Protection Authority has made it stricter that they must carry out a detailed mapping of the internal IT architecture and the IT environment in collaboration with the parties involved. Including a mapping of integrations between FMK and other source and recipient systems, so that it is clear what data responsibility the Danish Health and Data Protection Agency has in relation to the processing of personal data in FMK, and what responsibility other data controllers have for processing personal data in source and recipient systems. This also puts involved parties in a better position to identify and correct integration errors in cooperation with each other.

The Danish Data Protection Authority has also clarified that it is the data controller's responsibility to report a breach of personal data security to the supervisory authority when the data controller has ascertained a loss of integrity of personal data

in its own IT system - also in situations where the breach is caused by errors in the source and customer systems belonging to another data controller.

Also read the Norwegian Data Protection Authority's final letter to the Danish Health Data Agency here.

Notification of the registered

The Capital Region and the Danish Health Data Agency have, in continuation of both security breaches, made a health professional notification of the affected data subjects. In this connection, the Danish Data Protection Authority has drawn attention to the fact that a healthcare notification cannot easily be equated with a notification under data protection law in situations where there is a high risk for the affected data subjects. Notification in such situations must meet the requirements laid down in the data protection regulation.

1. Decision

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

At the same time, the Danish Data Protection Authority finds that there is a basis for issuing an order to the Capital Region to prepare and introduce a process that ensures that no changes to the health platform's functionality or data basis are implemented and put into operation before it is ensured that no known integrations with other systems create incorrect information in these. The order is shared in accordance with the data protection regulation, article 58, subsection 2, letter d. The deadline for compliance with the order is 10 March 2022. The Data Protection Authority must request to receive confirmation that the order has been complied with by the same date. According to the Data Protection Act[2] § 41, subsection 2, no. 5, anyone who fails to comply with an order issued by the Danish Data Protection Authority pursuant to Article 58, subsection of the Data Protection Regulation shall be punished with a fine or imprisonment for up to 6 months. 2, letters d and e.

The Danish Data Protection Authority must also issue a warning to the Capital Region that the commissioning of system changes in the health platform, where data integration with other systems occurs, without data integrity tests being carried out, is likely to be in breach of Articles 5, subsection 1 of the Data Protection Regulation. 1, letters a and d, 32, subsection 1. The warning is given in accordance with Article 58, subsection of the Data Protection Regulation. 2, letter a.

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

2. Presentation of the case regarding 2020-442-8862

On 10 August 2020, the Danish Health Data Protection Agency reported a breach of personal data security to the Danish Data Protection Authority.

It appears from the notification that a code change in the Health Platform, for which the Capital Region is the data controller, has resulted in an unintentional double prescription in the Common Medicine Card (FMK), for which the Danish Health Data Agency is the data controller, so that in the period between 16 July and on 10 August 2020, there was a loss of integrity of personal data in 4,223 medicine prescriptions concerning 2,310 registered persons.

It appears from the case that changes in an underlying hierarchy of rules, which were not directly related to the prescription of medicinal products and the communication thereof to FMK, have affected the technical set-up in the Health Platform such that in the period between 16 and 23 July 2020 an error occurred in the integration mechanism between the medicine module in the Health Platform and FMK.

It also appears from the case that the Capital Region became aware of the coding error on 17 July 2020 on the basis of a user inquiry and then carried out improvements on 23 July 2020. Following the incident, the region has been in dialogue with the Agency for Patient Safety and the hospital directorates and regional councils in the Capital Region and Zealand Region. In this connection, the Capital Region has stated that the region did not inform the Danish Health Data Agency about the incident by mistake.

2.1. Comments from the Danish Health Data Agency

The Danish Health Data Agency has informed the case that the integrity error in the information in FMK was discovered on 8 August on the basis of mention of the incident in the press. This resulted in 2,310 registrants receiving double prescriptions for medication in the period between 16 July and 10 August 2020.

2.2. Comments from the Capital Region

The Capital Region has informed the case that the region had the opportunity to test the communication and discover the error. However, there was no test of the communication between the Health Platform and FMK, as the coding error occurred in connection with a correction of an inappropriateness in a workflow in the Health Platform, which was not directly connected to the prescription of medicines and communication thereof to FMK.

It appears from the consultation response that, following the incident, the Capital Region has initiated work on qualifying relevant test scenarios and follow-up on procedures in order to better identify dependencies to FMK and then carry out the necessary tests before changes are put into production.

The Capital Region has also stated that the region has initiated a review of procedures to ensure that the FMK team at the Danish Health Data Agency is always contacted as soon as possible after identifying any similar incidents.

In conclusion, the Capital Region has stated that the region has assumed responsibility for notifying the registered in the period between 30 July and 27 August, where, according to a concrete health professional assessment, there could be said to be a patient safety consequence and thus a health risk for those registered. The specific healthcare assessment was carried out by staff in the patient-responsible departments, who were then in charge of contact and healthcare notification of the patients where this was deemed necessary.

3. Presentation of the case regarding 2021-442-13762

On 8 July 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 that a code error during an upgrade in the Health Platform has led to a discrepancy in the product descriptions for 164 item numbers (medicines). This erroneous information was shown in FMK so that in the period between 17 March and 30 June 2021 there was a loss of integrity of personal data in 1,311 drug prescriptions distributed among 1,149 patients from the Capital Region and Zealand Region.

It appears from the case that code changes made by the supplier of the Health Platform have resulted in the display of an incorrect prescription strength in the "Effectiveness" tab, as the drug file in question refers to an old version of the relevant product number file, which has affected the display of prescription strength of medicines in FMK.

It also appears from the case that the Capital Region became aware of the coding error on 22 June 2021 on the basis of a user inquiry and then corrected the error on 30 June 2021. In this connection, the Capital Region has stated that the region first became aware that the error affected FMK on 2 July 2021 and has informed the Danish Health Data Agency about the incident by email of 7 July 2021.

The region has informed the case that the supplier has not tested for this error in connection with the release of the update and has therefore not discovered that the code was faulty.

4. Reason for the Data Protection Authority's decision

On the basis of what the Danish Health Data Agency and the Capital Region have informed, the Danish Data Protection Authority assumes that integration errors between FMK and the Health Platform resulted in double prescribing of medicine.

On this basis, the Danish Data Protection Authority assumes that there has been an accidental change 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.

4.1. 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 mean that in socially critical systems with a large number of special categories of information about a large number of users, higher requirements are placed on the data controller to ensure that no there is an accidental change to personal data, which could have serious consequences for the data subjects.

As far as IT systems are concerned, for which the data controller is not itself responsible, but where the data controller is responsible for significant inputs in the form of personal data, the Danish Data Protection Authority is of the opinion that the requirement for adequate security will normally entail that the data controller must create the necessary overview of 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 controller has a duty to report code changes in integrated systems to relevant data controllers for the integrated external systems before they go into production. These requirements must ensure that external data controllers 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.

The Danish Data Protection Authority finds that a risk profile such as in these cases indicates that testing and quality control should have been carried out with regard to the impact of the code changes on the integrated systems, including testing of relevant test scenarios in order to be able to identify dependencies with other systems and then implement the necessary tests before the changes were put into production.

The Danish Data Protection Authority also considers that the data controller must ensure timely notification of all relevant data controllers in situations where errors have been detected in integrations between the systems.

Based on the above, the Danish Data Protection Authority finds that the Capital Region - by not having qualified relevant test scenarios in order to better identify dependencies to FMK, by not having carried out necessary tests before the changes were put into production, by not having informed the Danish Health and Data Protection Agency about the incidents immediately after the incidents finding – has not taken appropriate organizational and technical measures to ensure a level of security that matches the risks that arise in connection with processing activities via integrated IT systems with several independent data controllers, cf. the data protection regulation's article 32, subsection 1.

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

In this assessment, the Danish Data Protection Authority has placed particular emphasis on the fact that even minor code changes and code errors in the integrated systems can entail significant risks for the rights of data subjects, and that it appears from the cases that the data controller has not informed all relevant parties, in order to reduce risks for the registered

When choosing a response, the Danish Data Protection Authority has emphasized that the Capital Region is responsible for a platform that exhibits master/source data and services to another user system in the healthcare system (FMK), which is of decisive importance for citizens to receive the correct treatment and service based on fair data. The Danish Data Protection Authority has further emphasized the nature of the personal data and the period when the integrity of the personal data was compromised.

The Danish Data Protection Authority has also placed increasing emphasis on the repetitive nature of the breaches.

In addition, the Danish Data Protection Authority finds grounds to notify the Capital Region of an order to prepare and introduce a process that ensures that no changes to the health platform's functionality or data base are implemented and put

into operation before it is ensured that there are no known integrations with other systems incorrect information is created in these. The order is announced in accordance with the data protection regulation, article 58, subsection 2, letter d.

The Danish Data Protection Authority must also issue a warning to the Capital Region that the commissioning of system changes in the health platform, where data integration with other systems occurs, without data integrity tests being carried out, will probably be in breach of the data protection regulation's articles 5, subsection 1, letter a and d and article 32, subsection 1. The warning is given in accordance with Article 58, subsection of the Data Protection Regulation. 2, letter a.

4.2. 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.

It is the opinion of the Danish Data Protection Authority that a breach of personal data security, which entails a loss of integrity regarding information that is particularly worthy of protection, including information about health and medication prescriptions, basically entails a high risk for the rights of the citizens concerned, since loss of integrity of such information can entail serious health consequences for citizens.

The Danish Data Protection Authority has noted that the Capital Region has carried out a health professional notification of the affected data subjects.

In this connection, the Danish Data Protection Authority must draw the region's attention to the fact that if a breach of personal data security entails a high risk for the data subjects and thus entails an obligation to notify the affected data subjects, this notification must meet the requirements laid down in Article 34, paragraph 1 of the Data Protection Regulation .2, cf. Article 33, subsection 3, letters b), c), d), which is why a healthcare notification cannot be easily equated with a data protection legal notification of the registered.

The Danish Data Protection Authority must therefore make sure that notifications in cases of breaches of personal data security comply with the description requirements under data protection law.

[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 (ge - national regulation on data protection).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (the Data Protection Act).