Insufficient security measures at the Region of Southern Denmark

Date: 12-06-2020

Decision

Public authorities

For a number of years, there was potential access for 30,000 employees to more than 800,000 citizens' personal information.

The Danish Data Protection Agency expresses serious criticism and orders the notification of citizens.

2020-442-6448

Summary

Since 2013, the Region of Southern Denmark has used a network drive for temporary storage of documents that were to be linked to the region's Electronic Patient Journal (EPR). In 2017, the network drive and the temporary warehouse were expanded to cover all units in the Region of Southern Denmark. The purpose of the temporary storage was to qualify the documents and ensure their quality by adding meta-data and then archiving the documents in EHR. After processing, the documents should be automatically deleted from the temporary storage. However, a number of different factors could mean that individual documents were in temporary storage for up to a few months.

The network drive was not protected with sufficient access control, as all of the Region of Southern Denmark's approx. 30,000 employees had access to the drive and thus the documents. No mechanical registration (logging) of the access to the documents was performed.

All employees with a log-on to the region's network therefore had access to documents containing general, confidential and personal information of special categories, including information concerning children or particularly vulnerable groups, and registered with a protected address.

On this basis, the Danish Data Protection Agency expresses serious criticism of the Region of Southern Denmark's processing of personal data.

At the same time, given the large number of employees who have had access to the drive, the period when the opportunity has been there and the nature of the personal data, the Danish Data Protection Agency has determined that there is a high risk to the data subjects' rights. notify data subjects of the breach of personal data security.

The Danish Data Protection Agency states, among other things, in the decision that when the data controller has not been able

to determine whether a potential access has been exploited or not, it is not enough to close the access, but it is also necessary to inform the data subjects because the risk for them is assessed as high.

Decision

On 6 February 2020, the Region of Southern Denmark reported a breach of personal data security. The review has the following reference number:

941b32124259375be065efbf5d0b70ebdf5ef776

The Danish Data Protection Agency must initially state that the Personal Data Act [1] per. 25 May 2018 has been repealed and replaced by the Data Protection Regulation [2] and the Data Protection Act [3]. This decision has therefore been taken in accordance with the current rules.

As the breach of personal data security has included periods, even before the Data Protection Regulation applied, the Danish Data Protection Agency has included this in determining the sanction.

Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Region of Southern Denmark's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Ordinance. 1.

At the same time, the Danish Data Protection Agency finds grounds for issuing an order to the Region of Southern Denmark to notify the data subjects of the breach of personal data security. The injunction is granted pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter e.

The deadline for compliance with the order is 26 June 2020. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with, together with an anonymised copy of the notification. According to the Data Protection Act, section 41, subsection 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter e.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. Case presentation

It appears from the case that the Region of Southern Denmark since 2013 has used a residual record platform for temporary

processing of received documents that were to be stored in the file archive OnBase, which is linked to the Electronic Patient Record (EPR). In 2017, the use of the residual journal platform was extended to all Region of Southern Denmark's units. The purpose of the residual journal platform has been to qualify the documents and associate metadata, after which the documents were to be transferred to the EHR. The documents have contained general and confidential personal information, as well as personal information of special categories, including information concerning children or particularly vulnerable and registered with protected address, for about 800,000 registered.

The residual journal platform served as a temporary storage location before the information was transferred to the EHR system, after which it was deleted from the temporary storage. For various reasons, the system could not always process the information, which is why some of the information has been stored for longer in the residual journal platform than intended, typically a few minutes, but especially in connection with verification or deletion of files, documents have been able to stay longer time, up to a few months.

On 24 January 2020, the region was made aware that all its more than 30,000 employees have had access to the network drive, which i.a. contained the residual journal platform. Personal information about more than 800,000 unique people has been processed on the servers in question.

The Region of Southern Denmark has not notified the data subjects, referring to the fact that appropriate technical and organizational measures have been implemented to ensure that the high risk to the rights of those affected is probably no longer real and that it will also require a disproportionate amount of effort.

3. Region of Southern Denmark's comments

The Region of Southern Denmark has stated that even though the region has reported the breach, cf. the Data Protection Ordinance art. 33, in the region's view, this does not mean that there has been an “unlawful” access, and at the time of notification, the region has no knowledge of any occurrence of unlawful access to personal data on the residual journal platform.

The Region of Southern Denmark has stated about the Residual Record platform that it is used to handle and temporarily store documents that cannot be automatically added to the Electronic Patient Record (EPR). These may be test results, references, images, videos, correspondence, or anything else that is relevant to document. The documents must finally be stored in the file archive OnBase and when created, the document is linked to the EPR via a link. Via this link, users can open the documents.

In order to be able to use the documents, these must be qualified and in connection with the qualification, deletions, special clean-ups or breakdowns, it has happened that documents have been available for a longer period of time, a maximum of a few months.

Regarding the residual journal platform, the Region of Southern Denmark has further stated that the purpose of the temporary storage of documents is to fulfill the region's obligation to carry out journalisation. There have been no documents on the platform that should not be there, and no documents are accumulating on the platform over time.

Access to documents in the residual journal platform could be achieved if an employee connected a PC to the network drive and used the PC's built-in options to find the server's address and folder structure. The Region of Southern Denmark estimates that it would require a certain degree of IT knowledge to be able to perform this. It is not possible for the Region of Southern Denmark to state how many times a single document has been accessed. The region emphasizes that the documents are only on the platforms for a very short time before they are forwarded to OnBase and / or EPR.

On 24 January 2020, the Region of Southern Denmark, via a common mailbox, was made aware that there was a challenge with rights in OnBase and that everyone in the region's domain could access this file share. The message continued:… and there is cpr data available for all domain users created in the rsyd.net domain (+30,000 employees). Additionally, there is no logging of that access, so someone should ask the system owner to have this fixed as soon as possible.

The region used the following days to get an overview of the situation and found below that: It is stated that there is monitoring on the input folders and that these are reviewed from time to time. However, the monitoring is deficient, and does not live up to the requirements, as they only show who has accessed the server itself and a time - and nothing else.

The Region of Southern Denmark has reviewed logs for 3 months for the platform. These logs do not give an indication of unauthorized access, but support the view that those who have used the access have had a business purpose. The need for access follows from their work tasks. The Region of Southern Denmark thus finds it unlikely that there are persons without need who have had access to the documents. The region has no written decision to grant all of the region's more than 30,000 employees access to that network drive.

The Region of Southern Denmark has stated that at the same time as the breach, a task force was set up, which has since worked to focus on implementing appropriate technical and organizational measures, e.g. strengthening access control and reviewing the log of the residual journal platform.

In relation to the consequences of the breach for the data subjects, the Region of Southern Denmark has emphasized:

that there is a breach of confidentiality,

that the breach includes general personal data, CPR number and special categories of personal data,

that over 800,000 unique CPR numbers have been processed on the servers in question during the period,

that the breach has probably been due to the system's implementation (the first hospital unit used the system from 2013, and since then all units have been added),

that the data subjects are identifiable,

that it can not be ruled out, due to the high number of registered, that among the 800,000 people there are special registered, ie. children or particularly vulnerable (eg registered with a protected address),

that the possible consequences of the breach are identity theft.

The Region of Southern Denmark has stated in the notification of the breach on 6 February 2020 that:

Regardless of whether it is assessed that the risk for the data subjects' rights and freedoms has been / is high, no notification of victims will be given, as the Region has

Implemented appropriate technical and organizational measures (see above under measures)

Implemented measures to ensure that the high risk to the rights of those affected is unlikely to be real (user access control and logging)

As it will require a disproportionate amount of effort.

In connection with follow-up on the report of breaches of personal data security, the Region of Southern Denmark has stated that:

In order to clarify the application of the nature of the Data Protection Regulation. 34 - Notification of breach of personal data security to the data subject - The Region of Southern Denmark has made a concrete and reactive risk assessment of the breach, including its consequences and the probability. The Region of Southern Denmark has assessed the risk for those registered as low. The assessment is based in particular on the following facts:

that the platform has not been accessible via the open internet, but only internally in the region,

that the platform for the average user has not been easy to find,

that it has required expanded IT skills to find the platform,

that all employees are subject to a duty of confidentiality.

4. Justification for the Danish Data Protection Agency's decision

It follows from Article 32 (1) of the Data Protection Regulation 1, that data controllers and data processors, taking into account the current technical level, implementation costs and the nature, scope, coherence and purpose of the processing in question, as well as the risks of varying probability and seriousness of natural persons' rights and freedoms, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to these risks. As an example of relevant measures, the provision highlights e.g. ability to ensure continuous confidentiality and procedures for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security, in accordance with Article 32 (2); 1, letter b and letter d.

In continuation of this, the Danish Data Protection Agency is of the opinion that it follows from the requirement for appropriate security, cf. Article 32 (1). 1, that for i.a. municipalities and regions, it is particularly relevant that procedures have been established for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure treatment security. The Danish Data Protection Agency has emphasized that municipalities and regions process large amounts of personal data about many data subjects (citizens, patients and employees), including special categories of personal data, cf. Article 9, and that the risk for the data subjects must generally be assumed to be high in case of loss of e.g. confidentiality.

Periodic checks shall, as appropriate, also include checks on an organization's central IT infrastructure, including servers, networks and other IT infrastructure, which support access to primary administrative systems, such as journal systems, other critical case management systems and financial systems. In connection with this, it should be noted that lack of periodic inspection in the opinion of the Danish Data Protection Agency entails an unnecessarily high risk that insufficient or deficient security measures will not be identified in time.

In relation to the reported breach of personal data security, the Data Inspectorate assumes - based on the Region of Southern Denmark's own explanation - that the documents on the Region of Southern Denmark's residual journal platform were unjustifiably available to more than 30,000 employees authorized to the region's network. decision that all employees in the region should have access to it, that documents with personal data were processed on the platform for more than 800,000 people, including health information, that the documents have been available to employees who did not have a work-related

need, that nothing has happened logging that can document a possible use of the personal data, and that monitoring of the folders in the residual platform was sporadic and deficient and did not meet the requirements of a procedure for regular testing and assessment of the effectiveness of the technical and organizational measures to ensure processing security. As a result, the Region of Southern Denmark has not complied with the provisions of Article 32 (1) of the Data Protection Regulation. 1, letter b and letter d.

When choosing a sanction, the Danish Data Protection Agency has placed special emphasis on the fact that the breach included documents for a very large number of persons, that ordinary, confidential and personal data of special categories were processed, including information concerning children or particularly vulnerable e.g. registered with a protected address, that unauthorized access to this information has entailed a high risk to the data subjects' rights and freedoms, that all employees who were authorized to the Region of Southern Denmark's network - regardless of whether there was a work-related need - had access to the documents, and that insufficient technical and organizational measures had been taken to cover this breach of personal data security for 7 years.

As a mitigating circumstance, the Danish Data Protection Agency has emphasized that only employees who during the period have been authorized to the Region of Southern Denmark's network have been able to access the documents, that the employees are subject to confidentiality and that the risk profile reflects that the documents were in transit. available for a limited time.

An offense which the person concerned, in particular in view of its extent and extent, would, if the entire offense had taken place after the entry into force of the Data Protection Regulation, normally give rise to a fine, whereas the part of the offense which took place before the entry into force of the Regulation would not normally could give rise to fines.

After an overall assessment of the above criteria, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Region of Southern Denmark has not processed personal data with appropriate technical and organizational measures, cf. 1.

The Danish Data Protection Agency has made an assessment of the Region of Southern Denmark's decision not to notify the data subjects with reference to the fact that the documents have not been available to anyone other than employees in the region, that the documents have not been easy to find and required expanded IT skills to find these and that all employees are subject to confidentiality.

Considering that the documents on the Region of Southern Denmark's residual journal platform have inadvertently been available to more than 30,000 employees in the region for a period of 7 years, that documents with personal data for more than 800,000 people have been processed on the platform, that some of the documents have contained confidential personal data, as well as personal data of special categories, including information concerning children or the particularly vulnerable and registered with a protected address, that no registration has been made - including logging - of access to the data, that the Region of Southern Denmark can therefore not prove that the personal data has not been unauthorized persons 'knowledge and that the information has thereby escaped the control of the Region of Southern Denmark, the Danish Data Protection Agency finds that the risk to the data subjects' rights and freedoms is high, which is why the data subjects must be notified in accordance with Article 34 of the Data Protection Regulation.

In general - if one has lost control of whether the confidentiality of information has been compromised - it can not be said by stopping the vulnerability in question that the risk of misuse of the information that may have been accessed has diminished. Considering the large number of users with access to the information, the nature of the information and the period in question, the Data Inspectorate does not find that the Region of Southern Denmark has justified conditions which mean that no notification is required, especially as the subsequent measures have not ensured , that the risk to the data subjects' rights and freedoms is probably no longer real, cf. Article 34 (1) of the Data Protection Regulation. 3 liters a and b.

The Danish Data Protection Agency thus finds grounds for issuing an order to the Region of Southern Denmark to notify the data subjects of the breach of personal data security.

If the Region of Southern Denmark deems that it is not possible to make individual notifications to the data subjects, or that it will require a disproportionate effort to identify the 800,000 affected, the Data Inspectorate finds that notification can be made by public announcement or similar measure, if this takes place on a way to ensure that data subjects are informed in a similarly effective manner in accordance with Article 34 (2) of the Data Protection Regulation. 3, letter c

The injunction is granted pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter e.

The content of the notification to data subjects shall comply with the requirements of Article 34 of the Data Protection Regulation, thus describing in clear language the nature of the notified breach of personal data security and containing at least the information and measures referred to in Article 33 (2). 3, letters b, c and d.

The deadline for compliance with the order is 26 June 2020. The Danish Data Protection Agency must request no later than

the same date to receive a confirmation that the order has been complied with, together with an anonymised copy of the notification. According to the Data Protection Act, section 41, subsection 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter e.

The Danish Data Protection Agency notes that the Authority's decisions cannot be appealed to another administrative authority, cf. section 30 of the Data Protection Act. However, the Danish Data Protection Agency's decision may be appealed to the courts, cf. section 63 of the Danish Constitution.

[1] ACT No. 429 of 31/05/2000 on the processing of personal data, as last amended by Act No. 410 of 27 April 2017.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).