Violation of personal data security at the Region of Southern Denmark

Date: 17-07-2020

Decision

Public authorities

The Danish Data Protection Agency expresses serious criticism that the Region of Southern Denmark had not carried out the necessary risk assessment and testing during the development of an IT system, which led to unauthorized access to pregnant women's names and social security numbers.

Journal number: 2018-442-0026

Summary

The Danish Data Protection Agency has made a decision in a case in which the Region of Southern Denmark has reported a breach of personal data security. In the decision, the Danish Data Protection Agency has found grounds for expressing serious criticism that the Region of Southern Denmark's processing of personal data has not taken place in accordance with the data protection law rules.

The decision was made on the basis of lack of risk assessment of a treatment, lack of measures regarding development and testing, lack of timely documentation of the circumstances of the breach, and deficiencies in the completed notification of the data subjects. The breach concerned unauthorized access to 365 people's name, social security number and information about pregnancy.

The decision sheds light on how a lack of risk assessment and a lack of focus on known IT security issues in the development and testing of IT solutions can lead to breaches of personal data security, which could have been avoided.

The decision also sheds light on how the lack of detection and documentation of a security breach can affect the data controller's ability to comply with the rules in the Data Protection Regulation, in this case including the content of the notification of the affected citizens.

When a data controller uses a data processor as a system and operations provider, the circumstances of a breach will often be better known by the IT provider than by the data controller. But because the data controller must document the breach, avoid similar breaches in the future and possibly inform the citizens concerned, it is essential for compliance with the Data Protection Regulation that the data controller has mechanisms that ensure that a similar knowledge of the incident and understanding of

the circumstances of the breach is recognized and documented by the data controller.

Decision

The Danish Data Protection Agency hereby returns to the case where the Region of Southern Denmark on 25 May 2018 reported a breach of personal data security. In a questionnaire survey, lists of pregnant women's name and social security number were made available to unauthorized persons. The review has the following reference number:

273eb5e9fcb5e01a3fe2ba1c39c334d03b50b8b6

The Danish Data Protection Agency must initially state that parts of the reported breach of personal data security took place before 25 May 2018. In this connection, the Danish Data Protection Agency should note that the Personal Data Act was repealed on 25 May 2018 and replaced by the Data Protection Regulation [1] and the Data Protection Act [2]. . This decision has therefore been taken in accordance with the rules of the Data Protection Regulation. However, in determining the sanction below, the Danish Data Protection Agency has set out the rules that applied at the time of the processing of personal data in question and what the sanction would have been under these rules.

Decision

After 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 Regulation. 1, artikel 33, stk. 5 and Article 34, para. 2.

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

2. Case presentation

On 25 May 2018, the Region of Southern Denmark reported a breach of personal data security to the Danish Data Protection Agency.

It appears from the case that approx. 2000 people (pregnant women) were asked to fill out a questionnaire. The persons had the opportunity to see a list with the name and social security number of other persons who had also been asked to fill in the same questionnaire. Based on the content of the questionnaire and the context, it could be deduced that the persons on the list were pregnant. The list had been mistakenly placed on the server that the people in question had access to. Access to the list, however, presupposed that the persons had not yet completed the questionnaire and that the persons only used part of the received URL for the questionnaire.

Overall, 365 women's personal information was shown to unauthorized persons in this way. Logs indicated that six people out of the potentially approx. 2000 people got a list of names and social security numbers to see. Depending on the time of viewing, the list displayed contained between 19 and 200 people.

The Region of Southern Denmark has stated in the case that at the time of the finding of the breach of personal data security, there was no risk assessment in accordance with Article 32 of the Data Protection Regulation, which covered the processing in the system in which the breach of personal data security occurred.

The Region of Southern Denmark has further stated that errors in the allocation of user access have been a contributing factor to the breach of personal data security.

In connection with the information in the case, the Region of Southern Denmark has provided changing explanations regarding the facts of the breach of personal data security, including the nature of the breach in the form of information about what actions the user of the questionnaire had to perform to gain unauthorized access to the list of names and social security numbers. In this connection, the Region of Southern Denmark was forced to obtain new information from an external supplier in order to answer the Danish Data Protection Agency's questions about how the unauthorized access to personal information could be obtained.

The Region of Southern Denmark has made a notification, cf. Article 34 (1) of the Data Protection Regulation. 1, of those registered about the breach. The notification stated, among other things, that:

We are writing to you as we have become aware that your name and CPR number have been accessed by very unfortunate errors by others who, like you, have received an information form from the Department of Gynecology and Obstetrics D.

[...]

Unfortunately, parts of this list have by human error been available to other recipients if they clicked around the information form in a very specific, unfortunate way.

[...]

There has been no other information available than your name and CPR number, as well as the information that you have received mail in your e-box from OUH. ”

However, this description did not correspond with the region's information to the Danish Data Protection Agency during the processing of the present case, where the Region of Southern Denmark, among other things, has stated that - in addition to

information on name and social security number - there was access to information on pregnancy.

Justification for the Danish Data Protection Agency's decision

3.1 Article 32 of the Data Protection Regulation

It follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks involved in the data controller's processing of personal data.

On the basis of the information provided by the Region of Southern Denmark, the Danish Data Protection Agency assumes that personal data, including particularly personal data worthy of protection in the form of information on pregnancy and social security number, has been passed on to unauthorized persons.

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

Against this background, the Danish Data Protection Agency finds that the Region of Southern Denmark - by not having carried out a risk assessment in connection with the processing of personal data in question, and by failing to develop and test properly with a focus on processing security - has not taken appropriate organizational and technical measures for to ensure a level of security appropriate to the risks involved in the processing of personal data by the Authority, in accordance with Article 32 (2) of the Data Protection Regulation; 1.

The Danish Data Protection Agency is of the opinion that, as the data controller, it must be ensured that information about data subjects, including in particular personal data of a nature worthy of protection, does not come to the knowledge of unauthorized persons. Furthermore, the Authority is of the opinion that the data controller and / or data processor - depending on the circumstances - must ensure system development with a focus on IT security and appropriate testing of protection of personal data, in IT projects involving the processing of personal data.

3.2 Article 33 of the Data Protection Regulation

It follows from Article 33 (1) of the Regulation 5, that the data controller documents all breaches of personal data security, including the facts of the breach of personal data security, its effects and the remedial measures taken. This documentation must enable the supervisory authority to verify compliance with this Article.

It is the Data Inspectorate's assessment that the Region of Southern Denmark has not acted in accordance with Article 33 (1) of the Data Protection Ordinance. 5.

The Danish Data Protection Agency finds that the Region of Southern Denmark has not been able to adequately account for the facts of the breach of personal data security and its effects. In this connection, the Danish Data Protection Agency has emphasized that the Region of Southern Denmark has submitted changing explanations regarding the reason for the breach of personal data security and what it required to obtain unauthorized access to the personal data.

Against this background, the Authority is of the opinion that the Region of Southern Denmark has not complied with the requirement in Article 33 (1) in a timely manner. 5, and that the final coverage of the facts of the breach first took place in connection with the Danish Data Protection Agency's case processing.

3.3 Article 34 of the Data Protection Regulation

It follows from Article 34 (1) of the Regulation 1, that when a breach of personal data security is likely to involve a high risk to 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.

Of para. 2, it follows, inter alia, that the notification of the data subject in accordance with para. 1 must describe in clear and comprehensible language the nature of the breach of personal data security.

The Danish Data Protection Agency is of the opinion that breaches of personal data security concerning information worthy of protection, including information on social security numbers and pregnancies, in principle entail a high risk for the rights of the affected citizens, as exposure to such information can involve serious violations of citizens' privacy. .

The Danish Data Protection Agency finds that the Region of Southern Denmark's processing of personal data - by not informing the data subjects sufficiently about the nature of the breach of personal data security - has not taken place in accordance with Article 34 (1) of the Data Protection Regulation. 2.

In this connection, the Danish Data Protection Agency has emphasized that the notification to the data subjects stated that no information other than name and social security number had been exposed, despite the fact that information on pregnancy could also be deduced from the exposed information and the context in which the information was included. The Danish Data Protection Agency has further emphasized that the notification's description of the circumstances - in particular how an unauthorized person could gain access to personal data - did not correspond with the description that was ultimately given to

the Danish Data Protection Agency.

In connection with this, the Danish Data Protection Agency must note that such notifications must give the data subjects the opportunity to take the necessary precautions with a view to protecting themselves.

3.4 Summary

On the basis of the above, the Danish Data Protection Agency finds overall that there is a basis 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 Regulation. 1, artikel 33, stk. 5 and Article 34, para. 2.

[1] 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).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[3] See e.g. https://owasp.org/www-project-top-ten/ and https://owasp.org/www-community/attacks/Path_Traversal