

## Violation of personal data security at Randers Municipality

Date: 15-04-2020

### Decision

#### Public authorities

The Danish Data Protection Agency has expressed serious criticism of Randers Municipality's processing of personal data, as personal data has been published on the municipality's website, and as the municipality has not reported the incident in question or notified the affected citizens in accordance with the regulations.

Journal number 2019-442-4873

### Summary

The Danish Data Protection Agency has made a decision in a case where Randers Municipality has reported a breach of personal data security. In the decision, the Danish Data Protection Agency has found grounds for expressing serious criticism that Randers Municipality's processing of personal data has not taken place in accordance with the data protection law rules. In the decision, the Danish Data Protection Agency has emphasized that personal information of a nature worthy of protection has been published on Randers Municipality's website, including information on name and address protection and information on children's well-being, diagnosis and affiliation with special school.

In addition, the Danish Data Protection Agency has emphasized that Randers Municipality has not reported the incident as a breach of personal data security to the Danish Data Protection Agency within the deadline stipulated in the Data Protection Ordinance, and that the municipality has not complied with the content or time of notification of the affected citizens.

### Decision

The Danish Data Protection Agency hereby returns to the case where Randers Municipality on 1 November 2019 reported a breach of personal data security.

### Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that Randers Municipality's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Ordinance. 1, artikel 33, stk. 1 and Article 34, para. 1-2.

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

## 2. Case presentation

On 1 November 2019, Randers Municipality reported a breach of personal data security to the Danish Data Protection Agency. It appears from the notification that the municipality on 18 October 2019, at 10:00, became aware that 15 consultation responses with personal information were publicly available on the municipality's website.

The consultation responses provided information on name and postcode - including information on name and address protection - as well as information on children's well-being, diagnosis and affiliation with special school. Randers Municipality has clarified that in 11 of the consultation responses information appeared on families with children in special schools, and that in 4 of the consultation responses information appeared on persons with name and address protection.

Randers Municipality has stated that in some of the consultation responses, personal information appeared which it has not been possible for the municipality to identify, and that the municipality on the basis of this has not been able to make a final statement of affected persons. However, the municipality has estimated that 11 affected data subjects were under 18 years of age during the incident period.

The consultation responses were available on the municipality's website in the period from 17 October 2019, at 09:52 - where the first consultation response was uploaded on the municipality's website - until 18 October 2019, at 21:00, where all the information was removed from the municipality's website. The reason why the municipality first reported the breach to the Danish Data Protection Agency on 1 November 2019 is that the municipality lacked an overview of the extent of the incident. Randers Municipality has stated that before a person submits a consultation response, the person is - in 3 rounds - made aware that the consultation response may not contain personal information of a confidential and sensitive nature. The person is also made aware that the municipality's employees read and remove personal information of a confidential and sensitive nature before the consultation response is published, in the event that the consultation response contains this type of information.

In continuation of this, Randers Municipality has stated that the reason for the incident was that a number of the municipality's employees - in connection with reading the consultation responses - were not aware of which personal information may not appear in the consultation responses.

Randers Municipality has stated that the municipality - due to the nature of the breach - has chosen not to investigate the extent to which unauthorized persons have accessed the information during the period in which the information has been

publicly available on the municipality's website. In connection with this, the municipality has stated that it will be possible for the municipality to specify how many people have visited the page with the information in question, but that it will not be possible to specify whether the visitors have seen the information in question.

Randers Municipality has also stated that at the time of the notification, the municipality assessed that the risk for the data subjects' rights was not so high that the affected persons would be notified of the incident. The municipality has subsequently - and as a result of the Data Inspectorate's consultations with the municipality - made a new assessment, and has on this basis chosen to inform the persons whom they have been able to identify in the consultation responses and about whom sensitive personal information has been published. Notification was made on 20 January 2020. The municipality has emphasized in the assessment that before a person submits a consultation response, the person is made aware that the municipality - before publication - reads and deletes any information of a sensitive nature.

Randers Municipality has finally stated that as a result of the incident, the municipality will continue to read consultation responses before publication, and that the municipality's employees will be clarified which information must be deleted in high-risk consultation responses, ie. for example, hearings regarding the closure of special schools, where there is a risk that information of a confidential and sensitive nature will appear.

Justification for the Danish Data Protection Agency's decision

### 3.1.

Based on the information provided by Randers Municipality, the Danish Data Protection Agency assumes that 15 consultation responses with personal information have been publicly available on the municipality's website in the period from 17 October 2019, at 09:52, until October 18, 2019, at 21:00.

The Danish Data Protection Agency finds that in connection with what has happened, there has been a breach of personal data security, as personal information has been published on Randers Municipality's website, which has been available to everyone.

On this basis, the Danish Data Protection Agency finds that Randers Municipality has not implemented appropriate technical and organizational measures to ensure an appropriate level of security, cf. Article 32 (1) of the Data Protection Ordinance. 1.

The Danish Data Protection Agency has emphasized that the incident concerns information worthy of protection, including information on name and address protection and information on children's well-being, diagnosis and affiliation with a special

school. The Danish Data Protection Agency has also emphasized that the municipality has estimated that 11 of the data subjects affected were under 18 years of age during the incident period.

In this connection, the Danish Data Protection Agency should note that the handling of sensitive personal data places greater demands on the employees' diligence in connection with the handling of the personal data.

On this basis, the Danish Data Protection Agency finds grounds for expressing serious criticism that Randers Municipality's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has noted that Randers Municipality - before the incident - had instructed the municipality's employees in which personal data must be deleted in submitted consultation responses before they are published. In this connection, the Danish Data Protection Agency has noted that these instructions have not been followed in connection with the incident in question.

The Danish Data Protection Agency has also emphasized that the information has been available on the employee portal for a shorter period, from 17 October 2019, at 09:52, until October 18, 2019, at 21:00, corresponding to 1 day and 11 hours.

Furthermore, the Danish Data Protection Agency has noted that Randers Municipality will continue to read consultation responses before publication, and that the municipality's employees will be clarified which information must be deleted in high-risk consultation responses.

### 3.2.

The Danish Data Protection Agency also finds that Randers Municipality has not acted in accordance with Article 33 (1) of the Data Protection Ordinance. 1, to report the breach of personal data security to the Danish Data Protection Agency within the deadline stipulated in the provision.

The data controller must, without undue delay and if possible within 72 hours after he has become aware of a breach of personal data security, report the breach to the Danish Data Protection Agency. If the notification is not made within 72 hours, the notification shall be accompanied by a justification for the delay, in accordance with Article 33 (2) of the Data Protection Regulation. 1.

In the assessment, the Danish Data Protection Agency has emphasized what Randers Municipality stated that the municipality became aware of the breach on 18 October 2019, but that the municipality - due to a lack of overview of the extent of the

incident - first reported the breach to the Danish Data Protection Agency on 1 November 2019. has further emphasized that the municipality has not provided sufficient reasons for the notification not being made within the time limit of 72 hours.

In this connection, the Danish Data Protection Agency must note that if the 72 hours are exceeded, it must be because - for special reasons, which the data controller is able to explain in more detail - it was not possible for the data controller to make the notification before the deadline. .

The Danish Data Protection Agency must also note that when and insofar as it is not possible to provide the information together, the information may be communicated step by step without unnecessary further delay, cf. Article 33 (1) of the Data Protection Regulation. 4.

It follows from page 13 of the Danish Data Protection Agency's guidelines on handling breaches of personal data security from February 2018 that the data protection law rules recognize that data controllers do not always have all the necessary information about a breach 72 hours after they have become aware of it, as complete and in-depth information about the incident is not always available during the initial period. The regulation therefore allows for step-by-step notification. This means that a data controller - after an initial notification - can contact the supervisory authority again if the data controller becomes aware of additional relevant information about the breach. In this connection, the Danish Data Protection Agency must note that it is not sanctioned to report an incident that ultimately turns out not to be a breach.

On this basis, the Danish Data Protection Agency finds grounds for expressing serious criticism that Randers Municipality has not acted in accordance with the rules in Article 33 (1) of the Data Protection Ordinance. 1.

### 3.3.

Finally, the Danish Data Protection Agency finds that Randers Municipality has not acted in accordance with Article 34 (1) of the Data Protection Ordinance. 1, to notify the persons concerned without undue delay of the breach of personal data security. Where a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the controller shall without undue delay notify the data subject of the breach of personal data security in accordance with Article 34 (2) of the Data Protection Regulation. 1.

In the assessment, the Danish Data Protection Agency has emphasized what Randers Municipality stated that the municipality became aware of the breach on 18 October 2019, but only notified the affected persons on 20 January 2020. The Danish Data Protection Agency has further emphasized that Randers Municipality not seen to have documented that the notification was

made without undue delay.

The Danish Data Protection Agency has noted that at the time of the notification, Randers Municipality assessed that the risk to the data subjects' rights was not so high that the affected persons would be notified of the incident. The Danish Data Protection Agency has further noted that the municipality has subsequently - and as a result of the Danish Data Protection Agency's consultations with the municipality - made a new assessment, and that the municipality, on the basis of this, has chosen to notify the affected persons.

The Danish Data Protection Agency is of the opinion that breaches of personal data security concerning information worthy of protection in principle entail a high risk for the rights of the affected citizens, as exposure of such information may involve serious violations for the citizens, for example by violating the citizen's integrity.

The Danish Data Protection Agency finds that the breach is likely to involve a high risk to the data subjects' rights and freedoms, as the incident concerns information worthy of protection, including information about children, and that the information has been publicly available to all, without documenting the extent to which unauthorized persons have accessed the information.

On this basis, the Danish Data Protection Agency finds that Randers Municipality has not acted in accordance with the rules in Article 34 (1) of the Data Protection Ordinance. 1.

Finally, the Danish Data Protection Agency finds that Randers Municipality has not notified the persons concerned of the breach of personal data security in accordance with Article 34 (1) of the Data Protection Regulation. 2.

Notification of the data subject in accordance with Article 34 (2) of the Data Protection Regulation Article 33 (1) shall describe in clear and comprehensible language the nature of the breach of personal data security and shall include at least the information and measures provided for in Article 33 (1). 1 (b), (c) and (d).

In the assessment, the Danish Data Protection Agency has emphasized that Randers Municipality's notification to the affected persons does not contain a description of the probable consequences of the breach of personal data security pursuant to Article 34 (1) of the Data Protection Ordinance. 2, in conjunction with Article 33, para. 3, letter c.

On this basis, the Danish Data Protection Agency finds grounds for expressing serious criticism that Randers Municipality has not acted in accordance with the rules in Article 34 (1) of the Data Protection Ordinance. 1-2.