Security breaches should have been reported to the Danish Data Protection Agency

Date: 02-11-2020

Decision

Public authorities

The Danish Data Protection Agency criticizes the fact that Randers Municipality has not complied with the requirement for appropriate security measures in connection with an unintentional disclosure of information. The Authority also criticizes the fact that the municipality did not report the breach of security to the Authority and that the municipality had not notified the complainant of the breach without undue delay.

Journal number: 2020-32-1390

Summary

On the basis of a complaint, the Danish Data Protection Agency has expressed criticism that Randers Municipality - by sending an intended dismissal to a wrong employee - has not complied with the requirement for appropriate security measures. The proposed termination contained information about the complainant's health conditions and trade union affiliation.

Furthermore, on the basis of the complaint, the Danish Data Protection Agency has expressed criticism that Randers Municipality had not reported the security breach to the Authority, and that the municipality had not notified complaints about the breach without undue delay.

With regard to the lack of notification of the security breach, the Danish Data Protection Agency found that the breach had been reported to the Authority, as in the Authority's view the breach entailed a risk of complaints.

In this connection, the Danish Data Protection Agency emphasized that - given the document's confidential nature of the document and that the document contained information about the complainants' health and trade union affiliation - there had been a special risk of loss of reputation and confidentiality for complainants in connection with the intended dismissal was sent to another employee at the workplace.

It appears on the occasion of the decision that it is the Data Inspectorate's opinion that in relation to the assessment of whether such 'internal' security breaches must be reported to the Authority, importance must be attached to what information is in question and which employee has received the information. In the specific case, where the breach included information about

an intended dismissal as well as information about health and trade union affiliation, the Authority's assessment is that the breach must in principle be reported to the Authority, unless special circumstances apply. Special conditions will i.a. could be that the recipient of the information is a specially trusted employee who is used to handling such information about employees in the municipality.

Decision

The Danish Data Protection Agency hereby returns to the case, where complainants on 24 February 2020 have complained to the Authority about Randers Municipality's processing of personal data.

Decision

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

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 Randers Municipality on 15 November 2019 by mistake sent an intended termination of complaints containing information about name and address, trade union affiliation and health information to another of the municipality's employees.

In addition, it appears from the case that the employee who incorrectly received the information about the complainant was the complainant's colleague at the time, and that he or she was not in a particularly trusted position or was otherwise used to handling personal data about the municipality's employees.

2.1. Complainant's remarks

Complainants have generally stated that Randers Municipality has sent an intended termination of complaints to another of the municipality's employees, and that complainants became aware of this through the employee in question.

2.2. Randers Municipality's comments

Randers Municipality has generally stated that the municipality has by mistake passed on an intended termination of complaints to another of the municipality's employees. The error occurred when an employee came to journal the intended termination of complaints about another employee's case, as the employee had the two cases open at the same time. As a

result, the employee by mistake sent the intended termination of complaints to the other employee via e-Box on 15 November 2019.

In addition, Randers Municipality has stated that the municipality immediately contacted the other employee on 15 November 2019, when the municipality became aware of the error. In this connection, the municipality informed the other employee not to access what was sent and to delete it immediately.

Randers Municipality has also stated that all the municipality's employees have been taught how to use the systems, including how to journal properly. As a result of the incident, Randers Municipality is in the process of reviewing the available work letters and procedures to ensure that the organizational security measures are sufficient. In addition, Randers Municipality will investigate whether it is possible to set up additional technical measures that can reduce this type of human error.

When asked, Randers Municipality has stated that the municipality has not reported the breach of personal data security to the Danish Data Protection Agency in accordance with Article 33 of the ordinance. to a wrong employee, and that all municipal employees are subject to a duty of confidentiality.

At the request of the Danish Data Protection Agency, Randers Municipality has stated that the employee who incorrectly received the information about complaints was the complainant's colleague at the time, and that the employee was not in a particularly trusted position. However, the employee in question was used to handling personal data in relation to citizens within the elderly care, but not in relation to information about employees in the municipality.

In addition, Randers Municipality has stated that the municipality has notified complaints about the incident in connection with complaints on its own initiative contacting the municipality on 17 February 2020, when she became aware of the error. Randers Municipality then investigated the case further and sent subsequent complaints a written notification of the incident on 21 February 2020, where the municipality described and apologized for the incident to complainants, just as the municipality stated that the other employee has been asked to delete the information received, and that the case has been reported to the municipality's data protection adviser.

In this connection, Randers Municipality has stated that the municipality has not followed the municipality's internal procedures for breaches of personal data security, and that the notification of complaints in the municipality's assessment has not taken place without undue delay in accordance with Article 34 (1) of the Regulation. It is also the municipality's assessment that the content of the notification has not been in accordance with the requirements of Article 34 (1) of the Regulation. 2.

Justification for the Danish Data Protection Agency's decision

The Danish Data Protection Agency assumes that there has been a breach of personal data security (unauthorized disclosure of or access to personal information), as Randers Municipality has by mistake sent personal information about complaints to unauthorized persons.

Based on the information, the Danish Data Protection Agency also assumes that Randers Municipality became aware of the breach of personal data security on 15 November 2019, and that Randers Municipality has not reported the breach to the Authority pursuant to Article 33 (1) of the Regulation. 1.

3.1.

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.

Thus, the data controller 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 put in place to protect the data subjects against these risks. In this case, the data controller must ensure that employees who process personal data have received adequate instructions and the necessary guidance.

The Danish Data Protection Agency is of the opinion that the handling of special categories of personal data covered by Article 9 of the Regulation places greater demands on the employees' diligence in connection with the transmission of personal data, including ensuring that correct information is sent to the right recipient.

The Danish Data Protection Agency finds that Randers Municipality has not complied with the requirement to implement appropriate security measures in Article 32 (1) of the Data Protection Ordinance. 1.

In particular, the Danish Data Protection Agency has emphasized that Randers Municipality has not carried out appropriate quality control of the content of the submitted document and control that the document was sent to the right recipient, which has led to the municipality inadvertently sending information about complaints to another employee in the municipality, including information on the complainant's health conditions and trade union affiliation.

The Authority has noted that Randers Municipality is in the process of reviewing the available working letters and procedures to ensure that the established organizational security measures are sufficient.

3.2.

It follows from Article 33 (1) of the Regulation 1, that the data controller in the event of a breach of personal data security without undue delay, and if possible within 72 hours, must report the breach to the Danish Data Protection Agency, unless it is unlikely that the breach of personal data security entails a risk to natural persons' rights or freedoms. A risk to the rights or freedoms of natural persons includes i.a. discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy or any other significant economic or social inconvenience to the data subject.

The Danish Data Protection Agency's guide on handling breaches of personal data security mentions an example of a breach [2], where an HR employee by mistake sends pay slips and employment contract to an incorrect employee in the company, and where it is agreed that the employee in question deletes the received documents immediately after becoming aware of the error. In this connection, it appears from the example that in such a case the breach does not necessarily have to be reported to the Danish Data Protection Agency, and that the company can assess that the breach does not involve a risk for the data subject, given that it is an “internal ”Breach, and that the company has great confidence in the employee in question.

In the present case, the Danish Data Protection Agency finds that Randers Municipality has not complied with the requirement in Article 33 (1) of the Data Protection Ordinance. 1, to report breaches of personal data security to the Authority.

This is because it is the Data Inspectorate's assessment that in the specific case there is a breach of personal data security that is subject to notification.

The Danish Data Protection Agency is hereby of the opinion that the breach entailed a risk of complaints, which is why the exception in Article 33, para. 1 - according to which notification of breach may be omitted if it is unlikely that the breach of personal data security entails a risk to the rights of natural persons or liberties that may exempt from notification - is not met.

In this connection, the Danish Data Protection Agency has emphasized that - given the document's confidential nature of the document, and that the document contains information about the complainants' health and trade union affiliation - there has been a special risk of loss of reputation and confidentiality for complainants in connection with the dismissal. was sent to another employee at the workplace.

It is thus also the Data Inspectorate's assessment that the breach of personal data security in the specific case differs from the example described above from the Authority's guidelines on handling breaches of personal data security, including in that the

document in question - an intended termination - in the Authority's opinion has a more confidential in nature than employment contracts and payslips, on which the example of the guide is based.

The Danish Data Protection Agency is of the opinion that in relation to the assessment of the risk to the data subject's rights, and whether notification must be made to the Danish Data Protection Agency in such cases, importance must be attached to the information in question and which employee has received the information. In a case such as the present, where the breach included information about an intended dismissal as well as information about health and trade union affiliation, the Data Inspectorate is of the opinion that the breach will in principle be notifiable, unless special circumstances apply. Special conditions will i.a. could be that the recipient of the information is a specially trusted employee who is used to handling such information about employees in the municipality.

3.3.

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 the provision para. It follows that the notification of data subjects must describe in clear and comprehensible language the nature of the breach and contain at least the information and measures referred to in Article 33 (2). 3, letters b, c, and d.

The Danish Data Protection Agency finds that Randers Municipality has not without undue delay notified complaints about the breach, cf. Article 34 (1) of the Data Protection Ordinance. And that the notification has not been made in accordance with Article 34 (1) of the Regulation. 2.

In this connection, the Danish Data Protection Agency has emphasized what Randers Municipality stated that the municipality became aware of the breach on 15 November 2019, and that the municipality only made oral notification of complaints on 17 February 2020, followed by a written notification on 21 February 2020.

In addition, the Danish Data Protection Agency has emphasized that the content of the notification, in Randers Municipality's own assessment, has not been in accordance with the requirements in Article 34 (1) of the Regulation. 2.

Finally, the Danish Data Protection Agency has emphasized that the breach of personal data security includes a document of a confidential staff nature which, in addition to the information on intended termination of complaints, contains special categories of personal data covered by Article 9 of the Regulation. of the information internally in the workplace - as mentioned in section

3.2. - may involve a risk of loss of reputation and confidentiality of complaints.

3.4.

Overall, the Danish Data Protection Agency thus finds that there is a basis for expressing 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.

[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] Reference is made to page 37 of the Danish Data Protection Agency's guidelines on handling breaches of personal data security, which can be accessed on the Authority's website.