Serious criticism of the University of Southern Denmark's insufficient testing of software updates

Date: 12-05-2022

Decision

Public authorities

Serious criticism

Reported breach of personal data security

Treatment safety

Access control

Unauthorized access

In connection with a software update in the University of Southern Denmark's HR system, the rights management was reset, which meant that all 7011 employees at the university had access to view 417 applications. University had not adequately tested the software update prior to implementation and therefore only discovered the changed rights management afterwards.

Journal number: 2021-442-13989

Summary

The Danish Data Protection Authority has made a decision in a case where the University of Southern Denmark has reported a breach of personal data security.

The University of Southern Denmark (SDU) uses an HR system where employees can be assigned a role so that they can access applications. However, in connection with a software update, the system's rights management was reset, which meant that all employees at the University of Southern Denmark were given see access to the applications. According to SDU, this meant that a total of 7,011 employees had had potential access to applications from a total of 417 applicants. Of these, approx. 400 employees have an access-related need to be able to access personal data in the HR system. Furthermore, the university did not keep a log of access to the application material and could therefore not identify what had been accessed.

Inadequate testing

The university had not performed sufficient testing of the software update before it was implemented in the production system, and therefore only discovered the changed rights management.

SDU noted in the case that they were not aware that the update would make a change in the role management and for that

reason did not have the opportunity to carry out a 14-day test on the test system, which was otherwise the practice.

The Danish Data Protection Authority found that the data controller, as part of the development and adaptation of IT solutions for the processing of personal data, must test a solution in order to be able to identify and assess conditions that, e.g. may lead to changing or resetting previously selected settings. This is particularly important when it comes to a basic function such as rights management.

The responsibility of the data controller cannot be waived simply because the software supplier has not provided sufficient information about the scope of the update.

Against this background, the Danish Data Protection Authority expressed serious criticism.

1. Decision

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

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

2. Case presentation

On 5 August 2021, the University of Southern Denmark reported a breach of personal data security to the Danish Data Protection Authority.

It appears from the case that the University of Southern Denmark uses an HR system where employees can be assigned a role so that they can access applications. In connection with an update of the production system, the rights management was set to default settings, with which all employees at the University of Southern Denmark were given view access to the applications.

The University of Southern Denmark has stated about their rights management that employees are assigned a standard role and can have a role added to the hiring and assessment committee. In addition, it is possible to have additional roles added in connection with employment procedures and access management. Access was made according to each individual employment process. It follows from the case that people with the specific roles of hiring manager, member of the hiring committee and member evaluation committee all had full access to see applications from all postings.

In connection with one of the four standard qualification updates of the HR system, the rights management was mistakenly set

to default settings. With this, the previous management of rights was abolished. The result of this was that all employees at the University of Southern Denmark were given access to view applications that were previously reserved for employees assigned the access granting role. According to the University of Southern Denmark, this meant that a total of 7,011 employees had potential access to applications from a total of 417 applicants. Of these, approx. 400 employees have an access-related need to be able to access personal data in the HR system.

The University of Southern Denmark has stated that they have not carried out tests on the test system before the update came into force. This is justified by the fact that SDU was not aware that the update would make a change in role management. As SDU was not aware of this, they did not have the opportunity to carry out a 14-day test on the test system, which was otherwise practice. SDU further notes that Oracle – which supplies the software and performs the update – has not notified in their letters that the update would lead to the changes in the roles and their associated functions.

It appears from the case that the University of Southern Denmark does not keep a log of se access. SDU is therefore not able to check whether any employees have improperly accessed the applications in question. In addition, the University of Southern Denmark has not investigated whether access to the affected personal data has been utilized during the period. It is SDU's assessment that the information has a low degree of utilization and that the probability that it has been accessed is small. SDU further states that, on that basis, it is difficult to investigate whether anyone has utilized the knowledge they have gained by looking at the applications.

The University of Southern Denmark has informed the case that the incident began in week 29 (2021). The incident was detected on 2 August 2021 by SDU's own IT technician and completed on 5 August 2021. The affected personal data consists – in addition to the application material itself – of name, contact information, social security numbers and health information. The university has stated that the health information has been limited to that of relevance for an application process. The University of Southern Denmark has notified those registered on 1 March 2022.

It appears from the case that, with each subsequent quarterly update, the University of Southern Denmark will run tests on the test system before the quarterly update is run on the production system. This is to ensure that access – as in this case – is not mistakenly granted again.

In conclusion, the University of Southern Denmark notes that they are working on the process around the purchase of IT systems and the handling of security breaches based on this case. They further intend to implement better instructions

regarding applicants' exclusion of social security numbers in their applications.

3. Reason for the Data Protection Authority's decision

On the basis of the information provided by the University of Southern Denmark, the Data Protection Authority assumes that 7,011 employees have had unauthorized access to the personal data of 417 applicants for 14 days, including e.g. the application material itself, social security numbers and health information. The Norwegian Data Protection Authority finds that there has been a breach of personal data security, cf. Article 4, No. 12 of the Data Protection Regulation.

3.1. 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.

It is the opinion of the Danish Data Protection Authority that, as the data controller, you must ensure that information about registered persons, including information particularly worthy of protection, does not come to the knowledge of unauthorized persons.

The Danish Data Protection Authority is of the opinion that the requirement cf. Article 32 for adequate security will normally mean that data controllers, as part of the development and adaptation of IT solutions for the processing of personal data, must ensure that the solution is tested with a view to identifying conditions that may lead for accidental or illegal destruction, loss, alteration, unauthorized disclosure of or access to personal data.

Furthermore, the Danish Data Protection Authority is of the opinion that it is the duty of the data controller to have carried out an assessment of the processing that takes place in connection with the potential changes, including e.g. resetting or changing access rights, on the basis of an upcoming software update. It is the opinion of the Data Protection Authority that what the University of Southern Denmark stated about the University's lack of knowledge of the content and scope of the update cannot lead to a different result.

Based on the above, the Danish Data Protection Authority finds that the University of Southern Denmark – by not having tested the quarterly update before final implementation in the production system – has not taken appropriate organizational

and technical measures to ensure a level of security that suits the risks involved in the university's processing of personal data, cf. the data protection regulation, 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 University of Southern Denmark's processing of personal data has not taken place in accordance with the rules in the Data Protection Regulation, Article 32, subsection 1.

When choosing a response, the Danish Data Protection Authority has emphasized that a function – in the form of rights management, which fundamentally determines who has access to personal data – must be subject to such follow-up as ensures that the data controller is up-to-date with what consequences a upcoming update can and will cause. This is a basic prerequisite for adequate testing of the update and the possibility of mitigating any identified problems before the final implementation. The Danish Data Protection Authority has also emphasized that the University of Southern Denmark does not keep logs on view access to application documents and cannot thereby identify whether personal data has been used.

In addition, the Danish Data Protection Authority has emphasized that a large number of employees have had access to 417 registrants' application material, i.a. social security numbers and health information. Especially for internal applicants, such access poses an increased risk.

The Danish Data Protection Authority has emphasized, as extenuating circumstances, that the University of Southern Denmark has contributed to the clarification of the case and, upon ascertaining the breach of personal data security, quickly implemented measures that limited the exposure of information. In addition, the supervision has emphasized that the University of Southern Denmark has general guidelines for testing before final implementation of updates, and the limited duration of the incident.

The Danish Data Protection Authority has noted that the University of Southern Denmark intends to carry out a test on the test system with each subsequent quarterly update before it is run on the production system. In addition, the Data Protection Authority must strengthen that the University of Southern Denmark independently seeks out knowledge about the consequences of future updates, also despite the fact that the software supplier itself has provided more or less adequate information.

3.2. Summary

The Danish Data Protection Authority finds that there are grounds for expressing serious criticism that the University of

Southern Denmark's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

[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 (general regulation on data protection).