Kolding Municipality had not taken appropriate technical and organizational measures

Date: 22-04-2020

Decision

Public authorities

The Danish Data Protection Agency expresses serious criticism of Kolding Municipality, as the lack of control measures and the employees' access to personal data did not constitute appropriate technical and organizational measures.

Journal number: 2019-442-4365

Summary

The Danish Data Protection Agency has processed a case in which Kolding Municipality has since 2012 processed documents containing personal data in around 400,000 cases without taking appropriate technical and organizational measures. The Authority therefore expresses serious criticism of Kolding Municipality's processing of personal data, cf. Article 32 (1) of the Data Protection Ordinance. 1.

Kolding Municipality has used an ESDH system for a number of years. In connection with an upgrade of the system, the municipality's supplier changed the rights management to the underlying file structure, without the municipality being informed. The documents, which under normal circumstances could only be accessed through the ESDH system, were made available to all the municipality's 2,400 employees, provided you went directly to the document folder. This direct access to the documents was not logged.

Kolding Municipality has had annual audits of a selection of the IT systems used. The audit reports show that the municipality's overall management of IT security within the accounting area is satisfactory. The audits did not include a general review of the technical and organizational security measures for the storage of documents and the integrity of the network infrastructure or the procedures for regular testing, assessment and evaluation of the effectiveness of such measures.

In the period 2016-2018, the audits carried out had generally not looked at personal data protection or errors in the configuration of access rights, and no other control had been set up. In view of this and given the concrete lack of security on the document drive and access without logging to the documents, no appropriate technical and organizational measures had been taken.

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

1. Opinion

On 30 September 2019, Kolding Municipality reported a breach of personal data security.

As the incident in this case dates back to 2012, the Danish Data Protection Agency must initially state that the Personal Data Act per. 25 May 2018 has been repealed and replaced by the Data Protection Regulation and the Data Protection Act. This decision has therefore been taken in accordance with the rules of the Data Protection Regulation and the Data Protection Act.

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that Kolding Municipality has not processed personal data with appropriate technical and organizational measures, cf. Article 32 (1) of the Data Protection Ordinance. 1.

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 Kolding Municipality uses the ESDH system Acadre and has done so for several years. The municipality has stated that there are around 400,000 cases in the system and that the case documents are stored on a network drive. The cases include civil cases, family cases, personnel cases, property cases, subject cases, etc.

In connection with an upgrade in 2012, one of Kolding Municipality's suppliers made a change in rights management, so that the network drive - and thus the direct access to the case documents - was opened for approx. 2,400 employees. Incidentally, such direct access to the documents outside of Acadre was not logged.

Kolding Municipality had reportedly not been informed by the supplier of the change in question.

During a scan of the network on 17 September 2019, Kolding Municipality found that there was unauthorized access to the network drive in question. The unauthorized access was subsequently shut down.

Kolding Municipality has informed the Danish Data Protection Agency that it was not possible to ascertain the error during daily use, as users already have access to the documents through Acadre, that no internal scan of the network had been performed prior to the scan on 17 September 2019. open file drives, and that scanning for open drives on the network in the future will be part of the GDPR annual cycle and the municipality's work with the implementation of ISO27000 and ISO27701.

It also appears from the case that Kolding Municipality in 2016, 2017 and 2018 had audits performed by the auditing firm BDO. The audits were primarily related to general IT controls and IT systems of importance to the municipality's accounting and financial reporting and thus did not directly include Acadre or the municipality's IT infrastructure as a whole.

It thus appears, among other things. the following of BDO's audit report for 2018 on the audit of the municipality's internal IT controls, including inquiries regarding data protection legislation (section 8.1):

"We have not performed an audit to ensure that the municipality complies with data protection legislation, but we have asked the municipality to obtain an overview of the area and to ensure that there are no violations that will have a significant impact on the municipality. annual accounts. "

The same audit report also states in relation to the audit of the scope of the municipality's internal IT controls (section 9.1):

“The audit has included audits of the municipality's general IT controls and selected application controls for the IT systems that are important for the municipality's accounting and financial reporting.

We have organized the audit according to a rotation principle so that not all areas are audited to the same extent every year. In 2018, the audit covered the following areas:

Procedures and controls for the acquisition, change and maintenance of the municipality's central financial management system.

Access security to the financial management system, payroll system and the security system KSP-CICS, including user administration, user rights, access control and system administration.

Access security when accessing server rooms.

Outsourcing of central IT systems, including the municipality's own controls as well as obtaining and assessing auditor's statements from IT service providers.

The audit has also included requirements in accordance with the Executive Order on the municipalities' budget and accounting system, auditing, etc. in relation to IT use as well as elements of management audit within IT organization, IT policies and IT risk assessments. Furthermore, the audit has included a follow-up on established control deficiencies from last year. ”

In conclusion of the work performed (section 9.2), it appears from the auditor's report that:

“It is our opinion that the municipality has in all material respects implemented appropriate internal IT controls that help to maintain the integrity of the information and the security of data that the IT systems process in relation to accounting and financial reporting. Furthermore, it is our opinion that the municipality's overall management of IT security within the areas reviewed is satisfactory. ”

In connection with this, Kolding Municipality has i.a. stated that it is the municipality's opinion that the audit paints a true and

general picture of the municipality's security level, as the financial systems are an integral part of the same infrastructure that supports Acadre.

Justification for the Danish Data Protection Agency's opinion

It follows from Article 32 (1) of the Data Protection Regulation 1, that data controllers and processors, taking into account the current technical level, the 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 level of safety 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, 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 process large amounts of personal data on many data subjects (citizens 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 the event of loss of f .ex. confidentiality.

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

In relation to the reported breach of personal data security, the Danish Data Protection Agency has noted that the documents on Kolding Municipality's ESDH document server have inadvertently been available to the municipality's employees for a period of approx. 7.5 years outside the municipality's ESDH system, Acadre, that the documents have thus been accessible without access control and logging, and that the municipality became aware of the unintentional access in connection with an internal control.

The Danish Data Protection Agency has also noted that Kolding Municipality has, at least for the years 2016, 2017 and 2018, had an external audit carried out of the IT controls (and partly data protection) that will have a significant impact on the municipality's annual accounts.

On the basis of the material received from Kolding Municipality, the Danish Data Protection Agency assumes that Kolding Municipality has not carried out - or has had procedures for - regular testing, assessment and evaluation of the established measures in relation to the municipality's IT infrastructure with a view to to establish an appropriate level of security in relation to securing the rights and freedoms of natural persons.

The Danish Data Protection Agency thus finds that there are grounds for expressing serious criticism that Kolding Municipality has not processed personal data with appropriate technical and organizational measures, cf. Article 32 (1) of the Data Protection Ordinance. 1.

In continuation of the above, the Danish Data Protection Agency should note that the audited reports submitted - which show that the municipality's overall management of IT security in the accounting area is satisfactory - especially considering the scope of the audits, do not change the Authority's assessment that the municipality has not necessary control procedures to ensure the rights of data subjects.

The Danish Data Protection Agency has noted that Kolding Municipality will in future, among other things, will scan for open drives on the network as part of the GDPR annual cycle and the municipality's work with the implementation of ISO27000 and ISO27701.

The Danish Data Protection Agency hereby considers the case closed and does not take any further action.