Security breach in the FLIS system

Date: 22-09-2020

Decision

Public authorities

Journal number: 2019-431-0037

Summary

In December 2018 - February 2019, the Danish Data Protection Agency received a number of notifications from the country's municipalities regarding the Joint Municipal Management Information System (FLIS), which are operated by Kombit A / S. The purpose of the system is to provide management information to the municipalities, which on the basis of the information can make decisions concerning the municipality's operations on a database basis.

In connection with the delivery of data to the municipalities, Kombit A / S 'sub-data processor Netcompany A / S was mistakenly omitted a filter that was to limit the individual municipalities' access to only include data on the citizens that the municipality has the right to see in the data set (primarily the municipality's own citizens).

As a result of the error, it has been possible over a period of just over 4 months for selected employees in the municipalities, as well as for individual municipalities' suppliers of Business Intelligence, to illegally access social security numbers and employment-related information of up to DKK 4.2 million. citizens.

Decision

The Danish Data Protection Agency hereby returns to the case where 84 municipalities - due to an error in data extraction from the Joint Municipal Management Information System (hereinafter FLIS) - have unlawfully gained access to social security numbers and employment-related information of up to DKK 4.2 million. citizens.

Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that Kombit A / S 'processing of personal data has not taken place in accordance with the rules in Article 28 (1) of the Data Protection Regulation [1]. Article 32 (3) (f).

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

2. Case presentation

Kombit A / S operates FLIS, which is an infrastructure for benchmark and management information. FLIS is developed by Netcompany A / S, which is a sub-data processor for Kombit A / S.

In the period 14 December 2018 to 11 February 2019, the Danish Data Protection Agency has received a number of reports of breaches of personal data security from 66 municipalities relating to the same incident in the FLIS system.

In this connection, the Danish Data Protection Agency has received a number of documents from various data controllers, including statements that the data controllers have obtained from Kombit A / S, which is the data processor for the municipalities in question.

Furthermore, Kombit A / S has by e-mail of 1 March 2019 sent lists to the Danish Data Protection Agency of

the 74 municipalities that had an agreement with the Danish Agency for Labor Market and Recruitment (STAR) and were therefore data responsible in relation to the security breach

the 84 municipalities that have wrongfully had access to data in relation to the security breach.

2.1. About the incident

It appears from the case that an employee at Kombit A / S 'sub-processor Netcompany A / S, in connection with the delivery of data from FLIS to the municipalities, by mistake omitted a filter in the system that was to limit the individual municipalities' data to only to include the citizens that the municipality has the right to see in the data set (primarily the municipality's own citizens).

As a result of the error, 84 municipalities have gained access to social security numbers and employment-related information (eg about possible unemployment benefits and cash benefits) of up to DKK 4.2 million. citizens. Some municipalities use third-party suppliers of Business Intelligence (BI), which has therefore also had access to the information. These are the companies KMD A / S, Fujitsu A / S, LIFA A / S and INSPARI A / S.

Kombit A / S has stated that no data has been publicly available via the Internet or similar, but has only been available in a closed IT environment between FLIS and the municipalities' BI solutions.

It also appears from the case that the error, which has been present since the beginning of August 2018, was discovered on 12 December 2018. The error was discovered, as KMD A / S - by virtue of its function as a BI supplier for a municipality - examined the performance of the system and therefore drew a list of social security numbers in the dataset without further information. In doing so, KMD A / S found that the table contained a disproportionate number of citizens in relation to the municipality's size, after which the company drew Kombit A / S's attention to the matter.

Kombit A / S has stated that the error was not discovered as part of Netcompany A / S 'development or testing of the system, nor in connection with Kombit A / S' follow-up on tests of the system.

2.2. Types of personal information

Kombit A / S has stated that the unduly disclosed information can be found in a table referred to as DimDreamBorger, which contains the following fields:

DimDreamBorgerId (a random and non-meaningful artificial key that binds the table DimDreamBorger together with other tables in FLIS)

social security number

sex

marital status

origin

citizenship

four fields indicating whether the citizen receives resp. unemployment benefits, cash benefits, sickness benefits or early retirement

24 fields containing dates for so-called reset calls [2]

start date of integration program

end date of integration program

Kombit A / S has stated that the table DimDreamBorger is a list of citizens with associated properties, but that the table is generally not used independently by the municipalities and BI suppliers, as it serves as a look-up from another table called FactDream, which was not covered by error, and was thus limited to the correct information.

2.3. Extent of accidental access

Kombit A / S has stated that the use of data in FLIS usually takes place via the FactDream table, and that the missing filter has not affected the data in the FactDream table, so it is the company's expectation that the municipalities during normal use have not been in contact with wrongful data.

Furthermore, Kombit A / S has stated that the final feedback from the municipalities and their BI suppliers indicates that in only two municipalities has a person accessed the table in question with the incorrect data. Furthermore, a BI supplier, KMD A / S,

has been in contact with the incorrect data in connection with the error being discovered.

According to Kombit A / S, the other 96 municipalities and the municipalities' three other BI suppliers have announced that they have not opened the table with the incorrect data.

2.4. Measures taken

Kombit A / S has stated that the relevant security procedures were initiated after the incident with instructions on deleting data and collecting information in collaboration with the sub-data processor Netcompany A / S, the municipalities and the BI suppliers.

Furthermore, Kombit A / S has stated that the company has demanded from the sub-processor Netcompany A / S that the scope of tests be expanded with regard to each municipality's access to data in FLIS.

2.5. Data Processor Agreements

Via Lejre Municipality, the Danish Data Protection Agency has been sent a copy of the data processor agreement that the municipality has entered into with Kombit A / S.

Kombit A / S has stated that the data processor agreement with Lejre Municipality is representative of the data processor agreements entered into with the other municipalities, so that these are instances of the same template.

It appears from section 4 of the data processor agreement that

Kombit A / S - to the extent that Kombit A / S processes personal data on behalf of the municipalities - must secure the personal data via technical and organizational measures, as described in the Data Protection Ordinance as well as the Data Protection Act and Appendix 1.

Kombit A / S shall assist the municipalities in complying with their obligations pursuant to Articles 32-36 of the Data Protection Ordinance.

Kombit A / S guarantees - to the extent that Kombit A / S processes personal data on behalf of the municipalities - to provide sufficient expertise, reliability and resources to implement appropriate technical and organizational measures such that Kombit A / S 'processing of the municipalities' personal data meets the requirements in the Data Protection Regulation and ensures the protection of data subjects' rights. The safety measures must be documented at the request of the Municipality.

Furthermore, it appears from section 5 of the data processor agreement that Kombit A / S - when the processing of personal data for which the municipalities are data responsible is left to sub-data processors - is responsible to the municipalities for the

sub-processors' compliance with their obligations.

Finally, it appears from section 7 of the data processor agreement that Kombit A / S from 25 May 2018 - to the extent that Kombit A / S processes personal data on behalf of the municipalities - must implement all security measures required to ensure an appropriate level of security.

Justification for the Danish Data Protection Agency's decision

It follows from Article 28 (1) of the Data Protection Regulation 3, letter f, that the data processor shall assist the data controller in ensuring compliance with the obligations under Articles 32-36, taking into account the nature of the processing and the information available to the data processor.

It also follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller and the data processor must implement appropriate technical and organizational measures to ensure the continued confidentiality of processing systems and services.

In the opinion of the Danish Data Protection Agency, it follows from Article 32 (1) of the Data Protection Regulation 1, that data controllers and data processors, as part of the procedure for change management / release management for a system, must ensure that the changed system is tested for inconveniences that the change may have caused.

The Danish Data Protection Agency assumes that - as a result of an error in the setup of a filter in FLIS - there has been an unlawful disclosure of the types of information specified in section 2.2, which involves e.g. information on social security numbers and employment-related information on, for example, unemployment benefits and cash benefits, up to DKK 4.2 million. citizens.

Furthermore, the Danish Data Protection Agency assumes that Kombit A / S has not performed the necessary tests in connection with data extraction from FLIS, in order to be able to detect the incorrectly set up filter, which has led to the unlawful disclosure.

The Danish Data Protection Agency therefore finds that Kombit A / S in its function as data processor for the 74 municipalities has not complied with Article 28 (1) of the Data Protection Ordinance. Article 32 (3) (f), cf. Article 32, as the company has not implemented sufficient technical and organizational security measures against the personal data of up to 4.2 mill. citizens come into the hands of outsiders.

On the basis of the above, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that

Kombit A / S 'processing of personal data has not taken place in accordance with Article 28 (1) of the Data Protection Regulation. Article 32 (3) (f).

Due to aggravating circumstances, the Danish Data Protection Agency has emphasized that

Kombit A / S - on the part of the system that relates to extraction of data from FLIS to the individual municipalities - has not introduced basic tests that ensure that the municipalities only receive the necessary data, including that the individual municipalities only receive a quantity of data , which is meaningful in relation to the number of citizens living in the municipality

The incident is of a large scale, as information of up to DKK 4.2 million has been unlawfully passed on. citizens.

Due to mitigating circumstances, the Danish Data Protection Agency has emphasized that

The purpose of the municipalities' processing of personal data is to collect management information with a view to evaluating the municipality's operations, as opposed to, for example, specific case processing, whereby the potential consequences for the data subjects are seen to be low.

the disclosure of the information has been made to professionals who agree that the information must be treated with confidentiality;

Kombit A / S has implemented the necessary logging to be able to determine with certainty that the actual access to the information has been limited

Kombit A / S 'handling of the case and assistance to the data controllers, in the Authority's view, has been quick and sufficient.

[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] Lejre Municipality has informed the Danish Data Protection Agency that the term covers interviews that are zero in relation to rules for interview frequency, which appear from the Act on Active Employment Efforts. Reset interviews thus include job interviews, CV interviews, interviews about sick follow-up and integration interviews that take place at the job centers.