Safety hole in Schultz Expose

Date: 22-09-2020

Decision

Private companies

Journal number: 2019-431-0048

Summary

In October 2019, the Danish Data Protection Agency received notifications from a number of municipalities regarding the Schultz Expose, which is operated by J.H. Schultz Information A / S. The purpose of the system is to provide management information to the job centers in the municipalities, which on the basis of the information can make decisions concerning the municipality's operations on a database basis.

During a system update, a security component that was supposed to ensure that only the relevant information was available to users with access to the system was temporarily disabled. As the update - due to a process that could not be completed - did not proceed as expected, the security component was not reactivated as scheduled.

As a result of the error, it has been possible for selected employees in the municipalities to illegally access employment-related information about approx. 1.5 million citizens from other municipalities.

Decision

The Danish Data Protection Agency hereby returns to the case where users in a number of municipalities - due to an error in a planned release of a new version of Schultz Expose - have been wrongfully given access to employment-related information about approx. 1.5 million citizens from other municipalities.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that J.H. Schultz Information A / S '(hereinafter Schultz) 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

Schultz runs Schultz Expose, which is a management information system for the municipalities' job centers. The information

processed in the Schultz Expose originates, among other things. from Schultz Fasit, which is a case management system used at the job centers in a number of municipalities.

In October 2019, the Danish Data Protection Agency received reports of breaches of personal data security from 26 municipalities relating to the same incident in the Schultz Expose system.

On the basis of the notifications, the Danish Data Protection Agency has on 28 October 2019 chosen to start a case of its own operation against Schultz, which is the data processor for the municipalities in question.

By letters dated 8 November 2019, 20 November 2019 and 21 December 2019, Schultz has commented on the matter.

2.1. About the incident

It appears from the case that on October 4, 2019, Schultz made a planned technical release [2] of a new version of the Schultz Expose. As this was a technical release, during the update there was a need to deactivate the security component that provides the right access rights, so that users in the municipalities only have access to the information that is relevant to the municipality in question.

In the context of the update, changes were made to a database schema [3], the update attempted to reconstruct a large number of rows in the database tables in a single transaction. As this process was extremely extensive, the process "hung" in an unfinished state, so the security component was never automatically activated after the update.

As a consequence of the security component not being activated automatically after the update, it has been possible for users in the municipalities with SQL access to Schultz Expose Datawarehouse to extract data from all municipalities that use Fasit, except Odense Municipality, Aarhus Municipality and Copenhagen Commune.

Schultz became aware of the error when Syddjurs Municipality on 8 October 2019 at 16.09, Schultz pointed out that the municipality could extract data from the Schultz Expose about citizens who do not belong to Syddjurs Municipality.

Schultz has stated that the system was shut down after the inquiry from Syddjurs Municipality, and that the error had been rectified on 9 October at 10.30.

Furthermore, Schultz has stated that access to the system is via login with personal certificates and that access to the system is logged. Thus, Schultz has been able to establish that three named employees in three municipalities accessed the system during the period when the security component was deactivated, and that in two of the three cases, data sets were retrieved containing information about citizens who did not belong to the municipality in question. .

Finally, Schultz stated that the error was not detected during the update, as follow-up on the security component's automatic reactivation was not part of the release process.

2.2. Types of personal information

Schultz has stated that the information from the Schultz Expose, which has been wrongly exhibited to users in the wrong municipalities, is general, statistical information about the citizens' connection to the job centers, which under normal circumstances is pseudonymised. Schultz has further stated that for some users it has been possible to link social security numbers to the data in question in order to link data with other data sources.

Schultz has further stated that some of the table columns, i.e. types of personal information that users in the municipalities have been able to access are:

the gender of the citizen

the age of the citizen

citizenship

case types: the type of case a citizen is involved in, eg unemployment benefits, job clarification, etc.

target groups: type of citizen in the system, eg recipient of unemployment benefits, recipient of cash benefits, etc.

status: an information about the citizen's unemployment, eg fully unemployed, partially unemployed, etc.

activity types: type of activity for the citizen, eg flex jobs, company internships, ordinary jobs, etc.

places of activity: the individual companies or organizations that are responsible for a given activity

number of calls, type and time

number of absences, exemptions and durations of these in connection with activities

Schultz has provided an anonymized example of database tables that were illegally accessed. The Danish Data Protection Agency has reviewed the submitted material. The Authority's assessment is that this is personal data covered by Articles 6 and 9 of the Data Protection Regulation in pseudonymised form. The pseudonymisation consists of the individual citizen being represented by a 36-digit GUID (globally unique identifier).

2.3. Extent of accidental access

Schultz has stated that during the period when the security component was deactivated, three named users in three municipalities accessed the system.

A user in Vejle Municipality had logged in to the system, but did not download any data set. This has been confirmed by Schultz via e-mail.

Another user in Silkeborg Municipality retrieved a data set that contained information about citizens in other municipalities, but did not use the data in question.

A third user in Syddjurs Municipality retrieved a data set that contained information about citizens in other municipalities. After reviewing 5-10 citizens' information, the user found that it was information about citizens that did not concern Syddjurs Municipality. The user then used a filter to retrieve only the relevant information.

Schultz has stated that the municipalities have had unauthorized access to information regarding approx. 1.5 million citizens.

Finally, Schultz has stated that the company has followed up with the three municipalities in question, and ensured the deletion of the illegally accessed data. Schultz has submitted statements in good faith from the employees concerned that the information in question has been deleted from any local files and copies.

2.4. Measures taken

Schultz states that the following measures have been taken to avoid similar incidents in the future:

The script [4] for updating and releasing new versions has been adapted so that the processes will not stop in the future

The release procedure has been changed so that it must now be followed up that the security component has been reactivated, regardless of the type of release

In addition to manual controls, automatic status monitoring of various components, including the safety component, is introduced

2.5. Data Processor Agreements

The Danish Data Protection Agency has received a template for the data processor agreements that the municipalities have entered into with Schultz in relation to the current incident.

Section 4.3 of the Data Processor Agreement states that Schultz must secure personal data via technical and organizational security measures, as described in the Data Protection Regulation, cf. Annex 1. Annex 1 states, among other things: that Schultz must have formal change management procedures in place to ensure that any change is duly authorized, tested and approved prior to implementation. It is further stated that the procedure must be supported by an effective separation of functions and / or management follow-up to ensure that no individual can control a change alone.

It is also stated in Section 4.5 of the Data Processor Agreement that, in accordance with the Data Protection Regulation, Schultz must assist municipalities in complying with their obligations under Articles 32-36 of the Data Protection Regulation.
Furthermore, section 4.6 of the Data Processor Agreement states that Schultz must provide sufficient expertise, reliability and resources to implement appropriate technical and organizational measures such that Schultz's processing of municipalities' personal data meets the requirements of the Data Protection Regulation and ensures the data subject's rights.
Finally, Section 7.1 of the Data Processor Agreement states that Schultz must take all necessary security measures to ensure an appropriate level of security.

Justification for the Danish Data Protection Agency's decision

The Danish Data Protection Agency assumes that - as a result of an error where a security component was not reactivated after updating - there has been / has been unauthorized access to the types of information specified in section 2.2, which involves e.g. employment-related information on, for example, unemployment benefits and cash benefits, approx. 1.5 million citizens.
Furthermore, the Danish Data Protection Agency assumes that Schultz has not carried out the necessary follow-up on updating the Schultz Expose, in order to be able to detect that the security component, which was to ensure the correct access control, was not reactivated as planned.
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.
The Danish Data Protection Agency is of the opinion that the requirement pursuant to Article 32 for appropriate security will normally include

bear in mind that data controllers and data processors, as part of the change management / release management procedure for a system, must ensure that the changed system is tested for inconveniences that the change may have caused.
The Danish Data Protection Agency therefore finds that Schulz in his function as data processor for the 26 municipalities has

not complied with Article 28 (1) of the Data Protection Regulation. Article 32 (3) (f), cf. Article 32, as the company has not implemented sufficient technical and organizational security measures against the fact that personal data approx. 1.5 million citizens come into the hands of outsiders.

In the light of the above, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Schultz '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

Schultz did not have procedures - either manual or technical - to verify that the security component that was supposed to ensure access control to the Schultz Expose Datawarehouse was reactivated after the update was completed.

the incident has a large scope, as there has been / has been illegal access to information approx. 1.5 million 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, whereby the potential consequences for the data subjects are seen to be low, as opposed to, for example, specific case processing.

the information that has been unfairly accessed was pseudonymised

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

Schultz has implemented the necessary logging to be able to determine with certainty that the actual access to the information has been limited

Schultz's handling of the breach as well as follow-up with the municipalities, 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] Schultz has stated that it operates with two other types of releases where deactivation of the security component is not necessary.

[3] A database schema specifies a structure of the underlying objects in a database, including tables, views, etc.

[4] A script is a collection of source code written in a scripting language, which is a type of programming language in which the code is executed continuously by a so-called interpreter, as opposed to compiled programming languages in which the source code is compiled into an executable file.