Data processor's processing of personal data outside instructions

Date: 19-12-2019

Decision

Public authorities

A municipality reported a breach of personal data security to the Danish Data Protection Agency when a data processor had used an unapproved subcontractor. The Danish Data Protection Agency expresses serious criticism that the data processor's use of the subcontractor was not in accordance with the rules.

Journal number: 2019-442-3996

Summary

The Danish Data Protection Agency has made a decision in a case where Herning Municipality reported a breach of personal data security, as a data processor had transferred personal data to an unapproved supplier. The supplier to whom the data processor transferred personal data processed the data in unsafe third countries.

The Danish Data Protection Agency expresses serious criticism that the data processor's transfer of data to the supplier was in breach of the Data Protection Ordinance, according to which data processors may not make use of data processors without the prior approval of the data controller. In its opinion on the degree of criticism, the Danish Data Protection Agency emphasized that the information concerned a high number of data subjects, that the information included a personal identity number and that there had been unauthorized transfer of personal data to insecure third countries.

Decision

The Danish Data Protection Agency hereby returns to the case where Herning Municipality on 3 September 2019 reported a breach of personal data security to the Authority, as personal data has apparently been processed by a supplier that Herning Municipality has not approved as a sub-data processor.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that EG A / S 'processing of personal data has not taken place in accordance with the rules in Article 6 (1) of the Data Protection Regulation [1]. 1 and the Data Protection Act § 11, para. Article 28 (2) of the Data Protection Regulation Article 28 (10) And Article 44 (2). 1.

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

2. Circumstances of the case

It appears from the case that Herning Municipality uses the financial management system ØS Indsigt, which the municipality owns together with two regions and 10 municipalities, which together form the "Ownership". The system has been developed by the company EG A / S (EG), which is also responsible for the ongoing development, operation and maintenance. In the specific case, the municipalities and regions are data controllers, Ejerkredsen is the data processor and EG is the sub-data processor. The owners and EG entered into the sub-processor agreement on 1 November 2018.

The sub-data processor agreement states that the supplier (EG) may not make use of a sub-data processor, unless this is stated in the data processor agreement between Ejerkredsen and EG. Appendix 2 of the submitted sub-processor provides a list of specific approved sub-processors.

For the operation of the Service Desk System, which is affiliated with ØS Insight, the EG supplier uses ServiceNow, which is domiciled in the Netherlands but has group companies in the USA, India and Australia. ServiceNow does not appear as an approved sub-data processor in the sub-data processor agreement between Ejerkredsen and EG.

ServiceNow is responsible for the ongoing processing of support requests from members of the Ownership Circle regarding ØS Insight through the Service Desk System. ServiceNow is also responsible for implementing system updates, security updates, and security patches that are implemented globally for the Service Desk System. As a rule, only personal information about the support users' name and e-mail address is processed in the Service Desk System, but there may be other personal information in the system if this has been part of a support case. To ensure that personal information is not transferred to ServiceNow's offices outside the EU, EG has disabled a so-called "follow the sun" support function. In this connection, ServiceNow informed EG that when this support function was deactivated, personal data would not be processed by ServiceNow's offices in third countries.

On 12 August 2019, ServiceNow informs EG that ServiceNow, despite the deactivation of the “follow the sun” support function, cannot guarantee that personal data will not be processed in third countries, as ServiceNow's employees in e.g. India may be responsible for implementing global security updates to the Service Desk System.

On 20 August 2019, Herning Municipality will become aware via Ejerkredsen that EG uses the sub-data processor ServiceNow. Herning Municipality ceases to process personal data in the Service Desk from this time, while the municipality

together with the Ownership District tries to clarify whether there is a breach of personal data security. The municipality reports it as a breach of personal data security to the Danish Data Protection Agency on 3 September 2019.

The report states that the breach includes information on the name, date of birth, contact information and social security number of an estimated 500 citizens.

2.1. Herning Municipality's comments

Herning Municipality has generally stated that the municipality was not aware that EG used the sub-data processor ServiceNow, as this did not appear in the data processor agreement between Ejerkredsen and EG. In the municipality's opinion, EG has acted outside instructions when using the sub-data processor ServiceNow.

In connection with the notification of the breach, Herning Municipality has noted that the notification was delayed because the municipality and the Ownership Circle had to assess whether there was a breach of personal data security. When the municipality and Ejerkredsen became aware that personal data is processed in third countries by a sub-data processor that Ejerkredsen has not approved, and that the transfer basis is uncertain, the municipality reported the incident to the Danish Data Protection Agency as a breach of personal data security.

2.2. EC comments

EG has generally stated that there is no breach of personal data security, as there has been no accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

EG has further stated that Ejerkredsen could not have any doubt that EG used ServiceNow as a sub-data processor, as it appeared from the offer material and from the parties' discussions that EG would establish the SaaS solution Service Desk System operated by ServiceNow. EG has noted that there was an oversight on the part of both parties, as ServiceNow does not appear as an approved sub-data processor in the sub-data processor agreement.

According to EG, it is doubtful that personal data has been transferred to third countries, as ServiceNow's employees in third countries only implement system and security patches where, in EG's assessment, personal data covered by the contractual relationship between EG and The circle of owners. However, EG has not been able to assume with certainty that no personal data will be processed in connection with the implementation of these patches, but if processing were to take place, this is based on the Privacy Shield and the EU Commission's standard agreements, which are part of the data processor agreement that EG has entered into with ServiceNow. In this connection, EG has stated that, in EG's view, there is a sufficient basis for

the transfer of personal data to insecure third countries in the agreement between EG and ServiceNow.

Justification for the Danish Data Protection Agency's decision

On the basis of the sub-data processor agreement submitted by Herning Municipality between Ejerkredsen and EG, the Danish Data Protection Agency has assumed that the agreement requires specific approval of additional sub-data processors. Based on the information in the case, the Danish Data Protection Agency has also assumed that ServiceNow is not an approved sub-data processor in the contractual relationship between Ejerkredsen, which is the data processor for the regions and municipalities that are co-owners of the ØS Indsigt system and EG. EG has therefore acted outside instructions when passing on the personal information to ServiceNow. It is thus the Data Inspectorate's assessment that EG, by determining the purpose of the processing itself, is data responsible for the transfer of personal data, cf. Article 28 (1) of the Data Protection Regulation. 10.

The Danish Data Protection Agency has also assumed that the personal data has come to the attention of unauthorized persons, as ServiceNow has not been an approved subcontractor in the contractual relationship between Ejerkredsen and EG. The Danish Data Protection Agency thus finds that EG in its function as sub-data processor for the owners of ØS Indsigt - by passing on the personal data to a supplier who has not previously been approved in writing by the Ownership or the municipalities and regions - has violated Article 28 (1) of the Data Protection Regulation. And as data controller pursuant to Article 28 (2). Has not been authorized in accordance with Article 6 (1) of the Regulation. 1 and the Data Protection Act § 11, para. 2, to transfer the personal information to ServiceNow.

The Danish Data Protection Agency also finds that EG, by not having the authority to transfer the personal data to ServiceNow, also does not have the authority to transfer the personal data to third countries, cf. Article 44 (1) of the Data Protection Regulation. 1, as transfer may only take place if the conditions of Chapter 5 of the Data Protection Regulation are met, subject to the other provisions of the Regulation.

Against this background, the Danish Data Protection Agency finds grounds for expressing serious criticism that EG's processing of personal data has not taken place in accordance with the rules in Article 6 (1) of the Data Protection Regulation. 1 and the Data Protection Act § 11, para. Article 28 (2) of the Data Protection Regulation Article 28 (10) And Article 44 (2). 1.

At the level of criticism, the Danish Data Protection Agency has emphasized that there is a high number of data subjects concerned, that the information that has been wrongly passed on includes the data subjects' social security numbers, and that

personal data has also been transferred to insecure third countries. to.

The fact that EG has entered into a data processor agreement with ServiceNow and that this data processor agreement, in EG's assessment, ensures a sufficient basis for transfer to insecure third countries, cannot lead to another result, as EG's transfer of personal data to ServiceNow is not based on the Data Protection Regulation. non-compliance with Article 28 (1) 2 of the Regulation.

The Danish Data Protection Agency has noted that Herning Municipality does not currently use the Service Desk System, while negotiations are underway to insert ServiceNow as a sub-processor in the data processor agreement between Ejerkredsen and EG.

[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).