Reply to inquiry

Regarding intentional or unintentional transfers to third countries

Date: 29-03-2022

Decision

Private companies

Reply to inquiry

Data processor

Transfer to third countries

On the basis of a specific inquiry from KOMBIT, the Danish Data Protection Authority has considered whether there will be an accidental transfer to a third country, when it appears from the data processing agreement that the data processor reserves the right to hand over personal data on the basis of decisions from public authorities, including in third countries .

Journal number: 2022-212-3529

Summary

Shortly after the publication of the Danish Data Protection Authority's guidance on the cloud, KOMBIT approached the Danish Data Protection Authority with a specific question prompted by the guidance's section on the provision of information to authorities in third countries.

Specifically, it is about KOMBIT – which supplies the Aula system to the Danish municipalities – using Netcompany as a sub-supplier, which in turn uses Amazon Web Services (AWS) as a sub-supplier.

According to KOMBIT, the information is processed as a starting point within the EU/EEA, but it also appears from the data processing agreement between Netcompany and AWS that this can be deviated from if necessary to comply with the legislation or a binding decision from a public authority. The question is whether – if AWS brings the exception into play – it is an intentional or unintentional transfer to third countries. The answer is decisive for whether the municipalities must observe the requirements for transfers to third countries, or whether it is a question of appropriate processing security.

In short, in the eyes of the Danish Data Protection Authority, this will be an intentional transfer to a third country. Therefore, the municipalities must ensure that the rules on transfers to third countries are complied with when or if AWS makes such transfers in accordance with the instructions set out in the data processing agreement. At the same time, the Danish Data Protection

Authority is preparing for a further dialogue with KOMBIT about handling this issue.

Response to inquiry

1. The inquiry

On 10 March 2022, KOMBIT approached the Danish Data Protection Authority with a question about the transfer of personal data to third countries in connection with the use of Amazon Web Services ("AWS") as a data processor.

KOMBIT supplies the IT system Aula to the country's municipalities. Aula is the joint communication platform for employees, parents and students at the country's primary schools and day care facilities.

In its inquiry, KOMBIT has described the data processor construction, which is the basis for the delivery of Aula to the municipalities. Based on KOMBIT's description, the Norwegian Data Protection Authority has summarized the construction in Figure 1 below.

Furthermore, KOMBIT has stated that the data processing agreement has been concluded with Amazon Web Services EMEA Sarl, which is located in Luxembourg, just as KOMBIT has forwarded a copy of the data processing agreement.

In addition, KOMBIT has provided an overall more detailed account of the data processing agreement with AWS and has stated the following:

"When using AWS' services, the customer chooses which AWS region the data is to be processed in. An AWS region is a geographically defined collection of data centers. Aula is set up for the Ireland region, and AWS' data processing thus basically takes place within this region and thus within the EU/EEA.

In the attached AWS GDPR Data Processing Addendum (AWS standard data processing agreement), the following appears under point 12 "Transfer of Personal Data":

“12.1 Regions. Customer may specify the location(s) where Customer Data will be processed within the AWS Network, including the EU (Dublin) Region, the EU (Frankfurt) Region, the EU (London) Region and the EU (Paris) Region (each a "Region"). Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses.”

Although Aula is set up for the Ireland region, according to clause 12.1 of AWS's standard data processing agreement, data

may be transferred outside the selected region (and thus also potentially transferred to third countries) in the following situations:

If necessary for the provision of certain specific AWS services selected by the service user

If necessary to comply with legislation or binding regulatory requests

When reviewing the AWS services used, it has been established that no specific AWS services are used outside the selected region, and that therefore no transfer of personal data to third countries takes place in connection with the delivery of certain specific AWS services at Aula.

The question to the Danish Data Protection Authority is therefore limited to no. 2 and the meaning of the following wording in AWS' data processing agreement: "Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except […] as necessary to comply with the law or binding order of a governmental body.".

Questions

The Danish Data Protection Authority's guidance on the transfer of personal data to third countries from July 2021 (3rd edition) contains an example 10 on precisely the provision of personal data at the request of authorities in third countries.

In the example, it is stated that "If the data processor chooses to transfer personal data to the third country in violation of the data processing agreement, it will be an unintentional transfer, and this means that the data protection regulation's rules on transfer to third countries do not apply in relation to the data controller".

In the Norwegian Data Protection Authority's new guidance on cloud (March 2022), section 3.6 (especially example 14), this situation is also mentioned:

"As shown in section. 2 in the above example, the above-mentioned problem is thus, in the opinion of the Danish Data Protection Authority, a question of appropriate processing security, where you as the data controller i.a. must ensure that personal data does not inadvertently come to the knowledge of unauthorized persons. In this connection, you must be aware that if your (European) cloud supplier – as your data processor – meets a request from law enforcement authorities in a third country, this will be a breach of personal data security for you. This is because in that case there is an unauthorized disclosure of personal data to the relevant authority."

Can the Data Protection Authority confirm or deny whether it will be an accidental transfer, if the possibility of transferring personal data to authorities, including authorities in third countries, appears in the data processor's standard data processing

agreement, and whether the situation must be handled according to the rules on appropriate processing security, cf. section 3.6 in the Norwegian Data Protection Authority's guidance on the cloud?”

2. Answer

This appears from the data protection regulation's article 28, subsection 3, letter a, that a data processor may only process personal data in accordance with documented instructions from the data controller, including with regard to the transfer of personal data to a third country or an international organization, unless required by EU law or the national law of the Member States, which the data processor is subject to.

As KOMBIT has stated in its application to the Danish Data Protection Authority, the municipalities' instructions to AWS regarding the transfer of personal data to third countries can be found in the data processing agreement's section 12, from which the following appears:

“Regions. Customer may specify the location(s) where Customer Data will be processed within the AWS Network, including the EU (Dublin) Region, the EU (Frankfurt) Region, the EU (London) Region and the EU (Paris) Region (each a "Region"). Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses.” (Emphasis added by the Danish Data Protection Authority)

The Danish Data Protection Authority is of the opinion that there will be an intentional transfer of personal data to third countries for the municipalities if and to the extent that AWS meets a request from a public authority in a third country that includes personal data for which the municipalities are data controllers.

The situation thus does not correspond to the situation described in section 3.6 and example 14 of the Danish Data Protection Authority's guidance on cloud and example 10 of the Danish Data Protection Authority's guidance on the transfer of personal data to third countries. This situation concerns cases where a data processor, in breach of the data processing agreement, transfers personal data to one or more third countries.

In the current situation, the municipalities - in accordance with the data processing agreement that has been submitted to the Danish Data Protection Authority - instead instruct AWS to transfer personal data to public authorities to the extent that it is necessary to comply with "the legislation or a binding decision from a public authority". The instructions do not appear to be

limited in relation to which countries, including third countries, legislation or binding decisions may be in question.

Against this background, in the Data Protection Authority's view, the municipalities must ensure that the rules in Chapter V of the Data Protection Regulation are observed if or when AWS makes such transfers in accordance with the instructions.

In this connection, the Danish Data Protection Authority draws attention to Article 48 of the Data Protection Regulation. It follows from this that any judgment handed down by a court or tribunal and any decision made by an administrative authority in a third country that requires a data controller or a data processor to transfer or pass on personal data, can only be recognized or enforced in any way if it is based on an international agreement, such as a treaty on mutual legal assistance between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer under Chapter V of the Data Protection Regulation.

In other words, a judgment or decision by a court or administrative authority in a third country does not in itself constitute a valid basis for transfer.

For an example of a closer analysis and assessment of the transfer of personal data on the basis of judgments or decisions from a court or administrative authority in a third country, the Danish Data Protection Authority refers to the joint opinion of the European Supervisory Authority and the European Data Protection Board of 10 July 2019 to the European Parliament's LIBE committee. The statement describes the legal conditions for the transfer of personal data based on requests to the United States under the US CLOUD Act.[1]

In conclusion, the Danish Data Protection Authority notes that the situation referred to in section 3.6 and example 14 in the Danish Data Protection Authority's guidance on the cloud as well as example 10 in the Danish Data Protection Authority's guidance on the transfer of personal data to third countries relate to cases where data processors are not instructed to transfer personal data to third countries . In these cases, when delivering services, the data processor processes personal data exclusively within the EU/EEA, but may – for example in terms of its group structure – be met with requests from public authorities in a third country where the data processor's parent company is established. If the data processor accepts such information, personal data will be transferred to the relevant third countries.[2]

It is thus a fundamental prerequisite in this situation that the data processor is not instructed to transfer personal data to third countries - neither regularly nor ad hoc. Only in such cases can the data processor's possible compliance with requests from third country public authorities contrary to its promises and what appears in the data processor agreement be considered a

matter of adequate processing security according to Article 32 of the Data Protection Regulation.

If the data controller wishes to use a data processor who may be met with such requests, the data controller must be aware of the following three conditions:

Firstly, the data controller must make sure that the data processor ensures sufficient guarantees that the rules of the data protection regulation are complied with. In other words, the data processor must guarantee that the person in question will comply with the data protection rules. This appears from the data protection regulation's article 28, subsection 1.

Secondly, the data controller must ensure the necessary processing security, including that the data processor processes the information confidentially and does not make it available to unauthorized persons. This means that the data controller must assess the risk that the data processor – contrary to its promises and what appears in the data processing agreement – grants a request in accordance with the legislation of a third country. It follows from the requirements for adequate processing security in the regulation's article 32, subsection 1, and Article 28, subsection 3, letter c.

Third, the data controller must supervise its data processor. If the data controller becomes aware that the data processor acts in violation of the data processor agreement by transferring personal data to a third country against the data controller's instructions, the data controller must take immediate action against this. This appears from the data protection regulation's article 28, subsection 3, letter a, that the data processor may only process personal data according to documented instructions from the data controller, including as regards the transfer of personal data to third countries.

As a follow-up to the above, the Danish Data Protection Authority is happy to enter into a dialogue with KOMBIT about the handling of the mentioned problem. The Danish Data Protection Authority initially proposes to hold a meeting between the Danish Data Protection Authority, KOMBIT and the municipalities and is happy to receive a number of proposals for possible meeting times.

[1] EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en

[2] The Norwegian Data Protection Authority's guidance on cloud (March 2022), section 3.6.