Serious criticism of the Tax Administration in case of notification

Date: 22-09-2021

Decision

The Danish Data Protection Agency hereby returns to the case where the Tax Administration on 12 July 2021 reported a breach of personal data security to the Danish Data Protection Agency.

Journal number: 2021-442-13805.

The review has the following reference number: 4ebaba6f9e5136afa27cdd3e3c48ad51366eb6ac.

The tax administration subsequently sent a follow-up on the notification to the Danish Data Protection Agency. The follow-up has the following reference number: 3fbf36f3d582e3555039c234bd278526fb517f10.

Summary

The Danish Data Protection Agency has made a decision in a case where the Danish Tax Agency had reported a breach of personal data security to the Authority. The notification stated that the Danish Tax Agency had notified the citizen affected by the breach two days before the agency had reported the breach to the Danish Data Protection Agency.

However, the Danish Data Protection Agency received a follow-up on the notification from the Danish Tax Agency over a month later, in which the Agency informed the Authority that no notification had been given to the data subject, as described in the first notification - but only approx. 40 days later. The Danish Tax Agency justified it for late notification with "extraordinary circumstances during the holiday period".

In this connection, the Danish Data Protection Agency is of the opinion that a very basic purpose of the duty to notify data subjects is that the data subjects must be able to safeguard their interests if they are affected by a security breach. This is to prevent their rights or freedoms from being violated.

It is in continuation of this that the Data Inspectorate's view is that the Authority must be able to safeguard the data subjects' rights if there has been no (correct) notification of the data subjects - e.g. by ordering the data controller to notify the data subject (s).

The Danish Data Protection Agency therefore - in the processing of the specific case - placed special emphasis on the fact that neither the data subject nor the Authority were able to safeguard the data subject's rights if the data subject had not been notified of the breach of personal data security. Due to the incorrect information that appeared in the notification, the Danish

Data Protection Agency was of the belief that the data subject had been notified of the incident.

In addition, the Danish Data Protection Agency emphasis that it must generally be expected that public authorities have established appropriate procedures, guidelines and contingency plans that allow the authority to notify data subjects in accordance with the rules - regardless of whether employees are on holiday.

Against this background, the Danish Data Protection Agency expressed serious criticism that the Danish Tax Agency's processing of personal data had not taken place in accordance with Article 34 (1) of the Data Protection Ordinance. 1.

Decision

Following an examination of the case, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Tax Administration's processing of personal data has not taken place in accordance with the rules in Article 34 (1) of the Data Protection Regulation [1]. 1.

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

2. Case presentation

On 12 July 2021, the tax administration reported a breach of personal data security to the Danish Data Protection Agency. The notification states that a letter of tax approval sent by the Tax Administration on 12 April 2021, which contained identification information, information of a financial nature and information on social security numbers, had been sent to a wrong recipient by human error.

On 8 July 2021, the Tax Administration became aware that a breach might have occurred when the wrong recipient approached the Tax Administration to draw attention to the unintentional disclosure. After the Tax Administration had investigated the matter on the basis of the inquiry, the Tax Administration found on 9 July 2021 that there had been a breach of personal data security.

It further appears from the notification that the Tax Administration had notified the data subject concerned - whose information had been inadvertently disclosed - on 10 July 2021

On the basis of the notification, the Danish Data Protection Agency sent a final letter to the Tax Administration on 23 July 2021, stating that on the basis of the information available, the Authority would not take any further action in the case. In this connection, the Danish Data Protection Agency drew the attention of the Tax Administration to the fact that the assessment of the case could be resumed if, for example. new information emerged in the case.

On 20 August 2021, the Danish Data Protection Agency then received a follow-up on the notification from the Tax Administration. The follow-up showed that the Tax Administration - despite the fact that the Tax Administration had stated in the notification that notification of the data subject had taken place before the Tax Administration reported the incident as a breach of personal data security to the Danish Data Protection Agency - had not notified the data subject on 10 July 2021 , but that notification had only taken place on 18 August 2021.

The tax administration justified it for late notification with extraordinary circumstances during the holiday period.

On the basis of the Tax Administration's follow-up on the notification, the Danish Data Protection Agency has chosen to re-evaluate the case.

Justification for the Danish Data Protection Agency's decision

3.1. Article 34 of the Data Protection Regulation

It follows from Article 34 (1) of the Regulation 1, that when a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the data controller shall notify the data subject without undue delay of the breach of personal data security.

The Danish Data Protection Agency is of the opinion that breaches of personal data security regarding sensitive / particularly protected information, including some information of a financial nature, information on social security numbers and the combination of the information, as a starting point entail a high risk for the rights of the citizens concerned. serious violations for the citizens, for example by violating the integrity of the citizen.

It is the Data Inspectorate's assessment that in cases such as the present, where there is a special protection consideration in the processing of personal identity number information and information of a financial nature - and the combination of the information - notification must be made in accordance with Article 34 of the Data Protection Regulation. high risk to the data subjects' rights and freedoms, for example in the form of breaches of integrity and identity theft.

In this connection, the Danish Data Protection Agency is of the opinion that a fundamental purpose of the duty to notify data subjects of breaches of personal data security is that the data subjects must be able to safeguard their interests in order to avoid their rights otherwise being violated.

It is in continuation of this that the Data Inspectorate's view is that, in the event that (registered) the data subjects have not been notified (correctly), they must be able to safeguard the data subjects' rights, e.g. by requiring data controllers to notify the

data subjects. If it appears from a notification that the data subjects have been notified, even though this is not the case, the Danish Data Protection Agency will therefore not be sufficiently able to safeguard the data subjects' rights. The Danish Data Protection Agency will thus e.g. could not assess whether the data subject concerned has been - correctly - notified if, for example. the notification states that a notification has been made, even if this is not the case.

If the data subject is not able to exercise his rights himself, because the data subject e.g. has not been notified of an unintentional disclosure of information about the data subject, and the Danish Data Protection Agency cannot assess on the basis of a notification whether a notification has been or should be made, there is a risk that the missing notification may lead to insufficient observation of the interests of the data subject, which may ultimately lead to a violation of the data subject's rights or freedoms.

Therefore, in the opinion of the Danish Data Protection Agency, it is of crucial importance for the protection of the data subjects, their rights and their freedoms that information in a report of a breach of personal data security that the data subjects concerned have been notified is correct.

The Danish Data Protection Agency finds that the Tax Administration's processing of personal data - by not notifying the data subject of the breach of personal data security without undue delay - has not taken place in accordance with Article 34 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency has emphasized that the Tax Administration first notified the data subject of the breach of personal data security on 18 August 2021, approx. 40 days after the Tax Administration became aware of the breach on 9 July 2021.

In addition, the Danish Data Protection Agency has emphasized that a public authority's failure to notify without undue delay of data subjects affected by a security breach can generally not be justified by “extraordinary circumstances during the holiday period”. In this connection, the Danish Data Protection Agency's assessment is that it must be expected in particular that public authorities have established appropriate procedures, contingency plans and the like that enable adequate observance of the data subjects' rights, even though staff who are generally co-responsible for the authority's compliance data protection law obligations, vacation.

The Danish Data Protection Agency has also emphasized that the breach had been going on for approx. 3 months, when the Tax Administration became aware of it, which emphasized the importance of notifying the data subject (s) as soon as possible.

Finally, in choosing the degree of criticism, the Danish Data Protection Agency has placed considerable emphasis on the fact that incorrect information appeared in the notification of notification of the data subject, and that the incorrect information entailed an unnecessarily high risk for the data subject.

In a mitigating direction, the Danish Data Protection Agency has emphasized that there is one registered person and that the Tax Administration itself informed the Authority that no correct notification had been made of the registered person.

3.2. Summary

On the basis of the above, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Tax Administration's processing of personal data has not taken place in accordance with the rules in Article 34 (1) of the Data Protection Regulation. 1.

Appendix: Legal basis

Excerpt from 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 Regulation on data protection).

Article 2, para. This Regulation shall apply to the processing of personal data carried out in whole or in part by means of automatic data processing and to other non-automatic processing of personal data which are or will be contained in a register.

Article 33. In the event of a breach of personal data security, the controller shall, without undue delay and, if possible within 72 hours of becoming aware of it, notify the breach of personal data security to the supervisory authority competent in accordance with Article 55, unless this is unlikely; , that the breach of personal data security involves a risk to the rights or freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a reason for the delay.

PCS. 2. The data processor shall notify the data controller without undue delay after becoming aware of a breach of personal data security.

PCS. 3. The one in para. The notification referred to in paragraph 1 must at least:

describe the nature of the breach of personal data security, including, if possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned;

provide the name and contact details of the data protection adviser or another contact point where further information can be

obtained

describe the likely consequences of the breach of personal data security

describe the measures taken or proposed by the data controller to deal with the breach of personal data security, including, where appropriate, measures to limit its potential harmful effects.

PCS. 4. When and to the extent that it is not possible to provide the information in aggregate, the information may be communicated step by step without undue further delay.

PCS. 5. The data controller shall document all breaches of personal data security, including the facts of the breach of personal data security, its effects and the remedial measures taken. This documentation must enable the supervisory authority to verify compliance with this article.

Article 34. Where a breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, the controller shall without undue delay notify the data subject of the breach of personal data security.

PCS. The notification of the data subject in accordance with paragraph 2 of this Article. Paragraph 1 must describe in clear and comprehensible language the nature of the breach of personal data security and contain at least the information and measures referred to in Article 33 (1). 3 (b), (c) and (d).

PCS. It is not necessary to notify the data subject as referred to in paragraph 1. 1, if one of the following conditions is met:

the data controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the personal data affected by the breach of personal data security, in particular measures that make the personal data incomprehensible to anyone who has not authorized access to it, such as encryption

the data controller has taken subsequent measures to ensure that the high risk to data subjects' rights and freedoms referred to in paragraph 1 1 is probably no longer real

it will require a disproportionate effort. In such a case, a public announcement or similar measure must be taken instead, informing the data subjects in a similarly effective manner.

PCS. 4. If the data controller has not already notified the data subject of the breach of personal data security, the supervisory authority may, after considering the likelihood that the breach of personal data security involves a high risk, require the data controller to do so or decide that one of the conditions in PCS. 3 are met.

[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).