Violation of personal data security in the Danish Data Protection Agency

Date: 11-09-2020

Decision

Public authorities

The Danish Data Protection Agency expresses serious criticism that the Authority even for a period of time disposed of paper that should have been shredded as ordinary waste paper and that the breach was reported too late.

Journal number: 2020-442-8866

Summary

The Danish Data Protection Agency has now completed its processing of the Authority's breach of personal data security. The breach consisted in the fact that paper material, which contained confidential and sensitive information and which should therefore have been shredded, was accidentally disposed of as ordinary waste paper. The Danish Data Protection Agency has formally reported the breach to the Authority, but this did not happen within the deadline of no more than 72 hours after the breach was found.

The Danish Data Protection Agency - after the case has been discussed at a meeting of the Data Council - expresses serious criticism of the breach and the failure to meet the deadline.

The Danish Data Protection Agency has previously in a number of similar cases, where paper material has not been disposed of correctly, found no reason to express actual criticism, but merely found that the violations have taken place.

When the Danish Data Protection Agency expresses serious criticism in this case, the Authority has emphasized that the Authority has a special obligation to comply with the requirements that follow the authority's own area.

Decision

On 10 August 2020, the Danish Data Protection Agency's secretariat [1] reported a breach of personal data security. The review has the following reference number: 085c9904700e6a8aebe6edae2d8be011bb8ed652.

Decision

After a review of the case, and after the case has been considered at a meeting of the Data Council, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the secretariat's processing of personal data has not taken place in accordance with the data protection regulation [2]. Article 32, paragraph 1, and Article 33, para. 1.

Below is a more detailed review of the case and a justification for the decision.

2. The competence of the Data Inspectorate

In connection with the processing of the present breach of personal data security, the Danish Data Protection Agency has had occasion to consider whether the Authority has the necessary competence to process the case arising from the Danish Data Protection Agency's own circumstances, or whether the case could instead be left to another authority. the same considerations of objectivity and trust, such as asserts itself in relation to personal incapacity.

According to the Danish Data Protection Agency's assessment, however, the Authority does not have the option of leaving the processing of the case to another (independent) authority with similar professional competencies. In this connection, the Danish Data Protection Agency has also placed special emphasis on the fact that it is expressly provided by law that the Authority has the competence to process cases of breaches of personal data security, cf. section 27 of the Data Protection Act, cf. Article 32 and 33 (1) (a).

The Danish Data Protection Agency has - to meet e.g. trust considerations - a decision has been made that this decision must be published, just as the case has been discussed at a meeting of the Data Council.

3. Case presentation

In its notification, the Secretariat has stated that an employee of the Secretariat on 5 August 2020 found that physical documents - which should have been shredded because they could contain confidential and sensitive personal information - had been disposed of as ordinary paper waste. This is material that is otherwise stored electronically in the Danish Data Protection Agency's systems, but which in connection with the secretariat's case processing has been printed by the employees when they e.g. have had to discuss a case internally or proofread a draft letter or note.

It also appears from the case that during the preparation of the Data Inspectorate's move to new premises in Valby, the secretariat informed the landlord of the premises that the inspectorate needed a plastic container for waste paper to be shredded for disposal of the above-mentioned type of waste paper. However, such a plastic container for shredding was not set up, which was also followed up in the first instance. Due to internal misunderstandings, a plastic container for ordinary paper waste was instead marked as a shredding container, without it being checked whether it was such a container.

From the Danish Data Protection Agency's move into new premises on 3 February until 5 August 2020, the Authority's employees used the container in question for the disposal of waste paper that had to be shredded. For a period of approx.

three months (13 March - 15 June 2020), during which the Data Inspectorate's employees worked from home due to the Covid-19 situation, the employees, however, only to a very modest extent disposed of paper waste for shredding.

The secretariat has been informed that the plastic container has been emptied 2-3 times a week, after which the paper waste has been stored in a container in a locked rubbish bin. The contents of the room's two paper containers have been picked up on Tuesdays and Fridays, after which the paper has been sent for recycling - typically for cardboard, newsprint and the like.

In addition, it appears from the case file that the Secretariat, immediately following the finding that the waste paper in the plastic container in question was not - as assumed - shredded, but instead treated as ordinary waste paper, took measures to ensure that paper material for shredding in the future would be disposed of sufficiently safely, including i.a. when setting up a locked container in strong plastic applied the text "shredding" in the printer compartment.

It also appears that even though the Danish Data Protection Agency was already aware of the breach in question in practice, the secretariat formally reported the breach of personal data security to the Danish Data Protection Agency on 10 August 2020 via Virk.dk.

In this connection, the Secretariat has stated that it was a human error that the notification was not made within the 72-hour time limit provided for in Article 33 (1) of the Data Protection Regulation. 1.

The Secretariat has internally emphasized the importance of complying with the notification deadline, just as the Danish Data Protection Agency's internal procedures for handling security incidents, including breaches of personal data security, have been reviewed in order to ensure that notifiable breaches of personal data security are reported in time.

It also appears from the case that the secretariat has assessed that it is not possible to identify data subjects who are affected by the breach. The Secretariat has also not had the opportunity to identify how much material has been wrongfully disposed of as ordinary paper waste, just as it is unknown how much of the material has contained confidential and sensitive personal information.

In connection with this, the Secretariat has stated that there are no indications that personal information has come to the knowledge of unauthorized persons. However, it cannot be ruled out that the breach of personal data security is likely to involve a high risk to the rights and freedoms of natural persons, and the Secretariat has therefore notified any affected citizens, etc. through news on the Danish Data Protection Agency's website on 20 and 26 August 2020.

4. Justification for the Danish Data Protection Agency's decision

On the basis of the information in the case, the Danish Data Protection Agency finds that for a period of approx. 6 months has been a breach of personal data security, in accordance with Article 4 (1) of the Data Protection Regulation. 1, no. 12, as paper waste that contained confidential and sensitive personal information was not disposed of sufficiently securely, whereby it cannot be ruled out that unauthorized persons had access to the personal information contained in the material.

In this connection, however, the Danish Data Protection Agency has noted that the Authority's employees for a period of approx. three months (13 March - 15 June 2020) worked from home due to the COVID-19 situation and that during this period only to a very modest extent waste paper has been disposed of for shredding.

4.1. Article 32 of the Data Protection Regulation

Pursuant to Article 32 (1) of the Data Protection Regulation 1, the data controller shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the data controller's processing of personal data.

Thus, the data controller has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are put in place to protect the data subjects against these risks.

In this connection, the Danish Data Protection Agency is of the opinion that the requirement for appropriate security, e.g. implies that the data controller must continuously ensure that information about data subjects - including in particular information of a confidential and sensitive nature - does not come to the knowledge of unauthorized persons.

With regard to the disposal of paper material containing personal data of a confidential or sensitive nature, the Danish Data Protection Agency is of the opinion that the requirement for appropriate security will normally mean that such paper waste is destroyed (typically by shredding) and that the paper waste must be secured against unauthorized access. until the actual destruction is completed. It is also the Data Inspectorate's opinion that when e.g. If there are changes in the physical framework for the processing (including disposal) of personal data, the data controller should reassess any risks and, if necessary, check implemented security measures.

The Danish Data Protection Agency finds that the Secretariat has not taken appropriate organizational and technical measures to ensure a level of security appropriate to the risks involved in the Authority's processing of personal data, in accordance with Article 32 (1) of the Data Protection Regulation. 1.

In this connection, the Danish Data Protection Agency has emphasized that the secretariat, in connection with the move to

new premises - and thus in connection with the commissioning of new routines for waste paper disposal - should have checked that paper waste containing confidential and sensitive information was stored and disposed of properly.

The Danish Data Protection Agency has noted that the secretariat has subsequently initiated measures with a view to ensuring that paper material for shredding is disposed of sufficiently safely in the future, including e.g. when setting up in the printer compartment of a locked container in strong plastic applied the text "shredding".

4.2. Article 33 of the Data Protection Regulation

It follows from Article 33 (1) of the Data Protection Regulation 1, that the data controller in the event of a breach of personal data security without undue delay and if possible within 72 hours must report the breach to the Danish Data Protection Agency, unless it is unlikely that the breach of personal data security entails a risk to natural persons' rights or freedoms.

The Danish Data Protection Agency is of the opinion that the breach of personal data security in question is of such a nature that it should be notified to the Authority pursuant to Article 33 (1) of the Data Protection Regulation. 1.

As the secretariat became aware of the breach on 5 August 2020, the Danish Data Protection Agency can state that the secretariat - by first reporting the breach of personal data security on 10 August 2020 - has not complied with the deadline of 72 hours and that the notification has therefore not been made in accordance with Article 33 (1) of the Data Protection Regulation 1.

In this connection, the Danish Data Protection Agency has noted that the secretariat has internally emphasized the importance of meeting the notification deadline for the employee who was responsible for making the specific notification, just as the Danish Data Protection Agency's internal procedures for handling security incidents, including breaches of personal data security, have been reviewed. in order to ensure that notifiable breaches of personal data security are reported in time.

4.3. Article 34 of the Data Protection Regulation

Article 34 (1) of the Data Protection Regulation 1, it appears 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 notifies the data subject without undue delay of the breach of personal data security.

It also follows from Article 34 (1) of the Data Protection Regulation 3, letter c, that it is not necessary to inform the data subjects if 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.

After reviewing the case, the Danish Data Protection Agency finds that the secretariat has, to the extent necessary, complied with the requirement to inform the data subjects, cf. Article 34 of the Data Protection Regulation.

In this connection, the Danish Data Protection Agency has emphasized that the secretariat has published news about the breach on 20 and 26 August 2020 on the Danish Data Protection Agency's website. were targeted at the data subjects, just as i.a. in the nationwide media has been press coverage of the case. Furthermore, the Danish Data Protection Agency has noted that it has not been possible for the secretariat to identify the data subjects who are affected by the breach.

4.4. Summary

The Danish Data Protection Agency has dealt with a number of cases of a similar nature, where data controllers have not ensured that paper material that should have been shredded has been disposed of in this way, or where data controllers have not otherwise handled paper material while observing appropriate security measures, cf. Article 32 (1) of the Data Protection Regulation 1.

For example, the Danish Data Protection Agency has treated a case where a data controller had disposed of paper material that should have been shredded as ordinary waste paper in a container belonging to another data controller, and a case where a data controller had disposed of confidential paper material as ordinary waste paper that subsequently was blown out of a container and landed in adjacent streets. The Danish Data Protection Agency has also dealt with several cases where several data controllers - unintentionally - have had access to the same shredding containers.

In connection with the processing of these and other similar cases - with the exception of a single case - the Danish Data Protection Agency has not expressed actual criticism of insufficient security, but has instead only concluded that a breach has occurred and that the Danish Data Protection Agency character will not take further action. The one case where (serious) criticism was expressed concerned with paper material that should have been shredded, but which was disposed of as ordinary paper waste and found by an unauthorized person.

In the case of late notification of breaches of personal data security, in accordance with Article 33 (1) of the Data Protection Regulation. 1, the Danish Data Protection Agency has also in several cases - in combination with other types of (serious) breaches of personal data security - expressed ‘criticism’ or ‘serious criticism’.

After a review of the case, and after the case has been considered at a meeting of the Data Council, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that the Secretariat's processing of personal

data has not taken place in accordance with Article 32 of the Data Protection Regulation. PCS. 1, and Article 33, para. 1.

In this connection, the Danish Data Protection Agency has emphasized that the Authority - as a supervisory authority in the field of data protection - has a special obligation to observe and comply with requirements that follow from the authority's own area of responsibility.

The Danish Data Protection Agency hereby considers the case closed and does not take any further action in the case.

[1] It follows from Act no. 502 of 23 May 2018 on data protection § 27 that the Danish Data Protection Agency consists of a council and a secretariat.

[2] 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).