Security breach in Odense Municipality

Date: 11-09-2020

Decision

Public authorities

Journal number: 2020-442-7724

Summary

In May 2020, Odense Municipality reported a breach of personal data security to the Danish Data Protection Agency. The breach concerns a system that was put into operation in May 2019 - ie one year prior to the notification - where it is possible to apply digitally for a personal supplement or single benefit. In the system, it is possible to carry out an application on behalf of someone else, which is relevant, for example, when a healthcare professional applies on behalf of a patient.

The system was set up so that when a person completed an application on behalf of a citizen, and he or she used his or her personal NemID, the person's name, address and social security number were sent in a receipt to the citizen via Digital Post.

Decision

The Danish Data Protection Agency hereby returns to the case, where Odense Municipality on 12 May 2020 reported a breach of personal data security to the Danish Data Protection Agency. The notification and follow-up of 29 June 2020 have the following reference numbers:

4da291891ee119d908b25ab7ac2c7df15aa0ee7a

5190162b104f7bd0bef4b00806a921f49232fdf4

On 24 August and 1 September 2020, Odense Municipality answered questions from the Danish Data Protection Agency.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Odense Municipality's processing of personal data has not taken place in accordance with the rules in the Data Protection Ordinance [1] Article 32 (1). 1.

At the same time, the Danish Data Protection Agency finds that there are grounds for issuing an order to Odense Municipality to investigate whether information on data subjects' protected addresses has been unlawfully disclosed, and if so, to inform the data subjects concerned, cf. Article 34 (1). 1 and 2, and contact the recipients of the information in question with a request that

the information be deleted. The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2, letters d and e. The deadline for compliance with the order is 21 September 2020. The Danish Data Protection Agency must request confirmation of compliance with the order no later than the same date. According to the Data Protection Act [2] § 41, para. 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letters d and e.

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 May 2020, Odense Municipality reported a breach of personal data security to the Danish Data Protection Agency, which concerned that a person, e.g. a podiatrist, could fill in an application or an evaluation form on behalf of a citizen, and if this was done using a Personal NemID (instead of an Employee / Company NemID) it meant that the citizen received a receipt containing the name, address and social security number of the one who had completed the application / evaluation form. This happened in 51 cases over a period of 13 months.

It appears from the case that on 14 May 2019, a solution was commissioned through which it was possible to digitally apply for a personal supplement or single benefit. It was possible for others than the applicant himself to complete the application. If e.g. a podiatrist completed the application on behalf of the applicant, and a Personal NemID was used, which resulted in the podiatrist's name, address and social security number being sent in a receipt to the citizen (applicant) at Digital Post, so that the receipt ended up in the citizen's e-box .

Odense Municipality has in relation to how the error occurred, stated the following:

When preparing the digital solution, no attention has been paid to the fact that information about another party became visible to the applicant - ie that information about the person who applied on behalf of another / submitted information in a case (foot status) was sent in the form of receipt to applicant.

In relation to tests for e.g. IT-security stated that tests have been carried out, but no test environment has been used and tests have therefore been deleted. The municipality has thus not been able to submit documentation of what these tests were about.

In the notification and follow-up to the notification, Odense Municipality has stated that subsequently, on 5 May 2020, new measures have been implemented. Receipts are thus still sent to the citizen, but now only with the citizen's social security number and only with the name of the person completing the application. The website also draws attention to the fact that it is

the therapist who must complete the evaluation of foot status, and that the therapist must use a company / employee certificate.

It appears from the case that Odense Municipality, when updating the report on 29 June 2020 - 24 days after the incident was established - had not decided whether the affected persons should be notified of the breach. Asked, the municipality has stated that those affected were not notified per. August 24, 2020, because:

It is not immediately assessed that the violation will involve a high risk to the rights and freedoms of natural persons, so it is assessed that it has not been necessary to notify.

Odense Municipality has stated that the citizens who have received a receipt in their e-Box with someone else's personal information, have not been contacted with a view to having this information deleted. The municipality has justified this on the grounds that these are elderly citizens who have received help in connection with an application, and are not considered to have noticed that it was a civil registration number instead of a civil registration number, and which would have difficulty implementing a deletion of the transferred personal data. The municipality has also emphasized that they have not received inquiries from citizens who have received a receipt with personal information regarding another person in connection with the security breach.

Justification for the Danish Data Protection Agency's decision

On the basis of the information provided by Odense Municipality, the Danish Data Protection Agency assumes that personal information has been inadvertently passed on in the form of names, addresses and social security numbers to unauthorized persons.

On this basis, the Danish Data Protection Agency assumes that there has been an unauthorized transfer of personal data, which is why the Authority finds that there has been a breach of personal data security, cf. Article 4, no. 12 of the Data Protection Regulation.

3.1. Article 32 of the Data Protection Regulation

It follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is 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.

The Danish Data Protection Agency is of the opinion that, as the data controller, it must be ensured that information about data subjects, including information worthy of special protection, does not come to the knowledge of unauthorized persons.

Furthermore, the Danish Data Protection Agency is of the opinion that the requirement in Article 32 (1) of the Data Protection Regulation 1, on appropriate security means that data controllers and data processors, as part of the development and adaptation of IT solutions for the processing of personal data, must ensure that the solution is tested in order to identify conditions that may lead to accidental or illegal destruction, loss, change, unauthorized disclosure of or access to personal information.

The Danish Data Protection Agency finds that Odense Municipality - by not being aware of the processing that took place in receipts sent to citizens and by not testing sufficiently - has not taken appropriate organizational and technical measures to ensure a level of security that suits the risks , which is in the municipality's processing of personal data, cf. Article 32 (1) of the Data Protection Regulation. 1.

In this connection, the Danish Data Protection Agency is of the opinion that the implementation of a functionality whereby a person (who applied on behalf of another citizen) could use his personal NemID, should give rise to the functionality being tested and that a comprehensive test course could and should have identified the errors in question, except that in certain cases personal data was unlawfully stated in the receipt generated by the IT solution.

The Danish Data Protection Agency thus finds that there are grounds for expressing criticism that Odense Municipality's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation [3]. 1.

As a mitigating circumstance, the Danish Data Protection Agency has emphasized that the breach concerns a limited number of data subjects and a limited amount of personal data, and not data covered by Article 9 or 10 of the Data Protection Regulation.

On the basis of the information provided, it is the Data Inspectorate's assessment that the process concerning the development and testing of the IT solution in question is characterized by a lack of focus on the processing of personal data and the risks involved in the processing. The Authority therefore considers it relevant to recommend to the municipality to review its procedures for the development and testing of IT solutions with a view to addressing these matters to the extent

necessary.

The Danish Data Protection Agency has also noted that Odense Municipality, 24 days after the incident, had not yet decided whether the data subjects should be notified of the breach. The Authority finds that it should be possible to do this more quickly when the municipality was significantly earlier aware of what had happened at the breach. In this connection, the Authority must note that the purpose of the notification is to give the data subjects the opportunity to exercise their rights, and the opportunities can be reduced the longer the time elapses since the breach has occurred - depending on the circumstances of the breach.

3.2. 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 inform 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 concerning information worthy of protection such as social security number and address - if the address is protected - as a starting point entail a high risk for the rights of the affected citizens, as exposure to such information may involve serious violations. the integrity of the citizen.

As the case is stated, Odense Municipality is not seen to have investigated whether some of the affected addresses are protected under the Civil Code Act. The Danish Data Protection Agency also assumes that Odense Municipality has decided not to notify the data subjects and not to contact the recipients of the information in question with a request that the information be deleted.

The Danish Data Protection Agency considers that it may pose a high risk if protected addresses have been accessible to unauthorized persons, and in this connection the Authority cannot rule out that disclosure of any information about protected addresses in the case in question will also pose a high risk for the data subjects. .

The Danish Data Protection Agency therefore finds that there is a basis for Odense Municipality to investigate whether some of the affected addresses are protected in order to assess whether the breach can potentially involve a high risk for individual affected persons, cf. Article 34, subsection. 1.

4. Order

The Danish Data Protection Agency therefore finds grounds for issuing an order to Odense Municipality to investigate whether

information on the data subjects' protected addresses has been unlawfully passed on and, if so, notified the data subjects concerned, cf. Article 34 (1). 1 and 2, and contact the recipients of the information in question with a request that the information be deleted. The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2, letters d and e.

The content of any notification to data subjects shall comply with the requirements of Article 34 of the Data Protection Regulation, thus describing in clear language the nature of the notified breach of personal data security and containing at least the information and measures referred to in Article 33 (2). 3, letters b, c and d.

The deadline for compliance with the order is 21 September 2020. The Danish Data Protection Agency must request no later than the same date to receive a confirmation that the order has been complied with. According to the Data Protection Act [4] § 41, para. 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letters d and e.

[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] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[3] 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).

[4] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).