Criticism of the municipality's IT system

Date: 11-01-2022

Decision

Public authorities

Criticism

Supervision / self-management case

Treatment safety

The Danish Data Protection Authority criticizes the fact that in certain cases it was possible to access information on who had last edited or ordered waste containers as well as any contact information in the IT system "Affaldsweb".

Journal number: 2021-432-0077

Summary

Based on a citizen's inquiry, in December 2021 the Data Protection Authority initiated a case of its own initiative against Herning Municipality.

In the decision, the Danish Data Protection Authority criticizes that the municipality's processing of personal data via the municipality's IT system "Wasteweb" until 17 December 2021 has not been done in accordance with the rules in the data protection regulation.

The users of "Affaldsweb" log into the system with a unique code of 5 digits/characters, which appears on their property tax ticket.

Until 17 December 2021, it was possible for citizens who shared a waste container to access information about who had last edited or ordered containers as well as any contact information that the previous user may have entered in "Waste Web".

It also follows from the case that the system makes it possible to search for information about a physical address as well as information about container conditions (volume, emptying frequency, price) at this address by URL manipulation. The user's unique code of 5 digits/characters is included in the URL and by manually changing it, it is thus potentially possible to access information about other users.

In this connection, the Danish Data Protection Authority has stated that an access protection based on a code with 5 digits/characters does not provide adequate security against attacks based on brute force and randomized guesses, and that

the use of consecutive numbers/letters or recognizable sequences of characters in the URL , which is used for individualized access, is not an expression of adequate protection.

The Danish Data Protection Authority has guided the municipality that information about addresses and container conditions combined with other identifiers can relatively easily become information that can be attributed to a person - i.e. personal data.

As far as the current set-up is concerned, the municipality has stated that the processing was of a less sensitive nature and that the service to the citizen exceeds potential risks for the rights of the data subjects.

To this, the Danish Data Protection Authority noted that all personal data is worthy of protection and that URL manipulation is a type of programming error source that is widely known and should be easily countered by the data controller. In addition, the supervisory authority pointed out that the balance between the less sensitive nature of the information on the one hand and the useful value of the service on the other hand cannot lead to any other result than that the personal data is worthy of protection.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing criticism that Herning Municipality's processing of personal data via the IT system: "Affaldsweb" until 17 December 2021 has not been done in accordance with the rules of the data protection regulation [1 ] article 32, subsection 1.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

It appears from the case that, until 17 December 2021, it has been possible - via Herning Municipality's IT system "Waste Web" - to access information about who last edited or ordered containers, as well as any contact information that the user himself may have entered in the relevant IT system.

Herning Municipality has informed the case that the information has been possible to access in situations where a waste container is shared by several citizens and where the user has been in possession of a 5-digit code that has been printed on the user's property tax ticket.

In addition, Herning Municipality has stated that - even without this code from the property tax ticket - it has been possible to see which waste containers have been associated with a specific address.

Finally, it follows from the case that the system per today makes it possible to search for information about a physical address as well as information about container conditions (volume, emptying frequency, price) at this address by the user manually

changing the identifiers in the URL address.

By changing the identifiers in the URL address, it is thus per today possible for users to access other addresses' container information.

In this connection, Herning Municipality has stated that the municipality has assessed that the processing is of a less sensitive nature, as it relates to container information on addresses, and that the service to the citizen exceeds potential risks for the rights of the data subjects.

3. Reason for the Data Protection Authority's decision

It follows from the data protection regulation article 32, subsection 1, that the data controller must 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.

The data controller thus 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 introduced to protect the data subjects against these risks.

The Danish Data Protection Authority is of the opinion that the requirement, cf. Article 32, for adequate security will normally entail that you as the data controller ensure that information about registered persons does not come to the knowledge of unauthorized persons.

3.1 The security of the IT system before 17 December 2021

Based on the information provided by Herning Municipality, the Danish Data Protection Authority assumes that it has been possible for unauthorized persons to access information about who last edited or ordered containers as well as any contact information that the user may have entered into the relevant IT system. until 17 December 2021, in cases where a waste container has been shared by several citizens and where the user has been in possession of a code with 5 digits/characters that has been printed on the user's property tax ticket.

Based on this, the Danish Data Protection Authority finds that Herning Municipality has not implemented appropriate technical and organizational measures to ensure an appropriate level of security, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has thereby emphasized that unauthorized persons have been able to access the information other users have entered into the system, of which other people's contact information may have been entered.

The Norwegian Data Protection Authority has also placed emphasis on the possibility that unauthorized persons have been able to access it

the information is due to a lack of technical measures that could prevent other users from becoming familiar with the personal data. The Danish Data Protection Authority is of the opinion that an access protection based on a code with 5 digits/characters does not provide adequate security against attacks based on brute force and randomized guesses, in addition the use of consecutive numbers/letters or recognizable sequences of characters in the URL that is used for individualized access, not an expression of adequate protection in access to personal data.

3.2 The security of the IT system per today

As far as the current set-up of the IT system is concerned, including the function that enables other users – by changing the identifiers in the URL address – to search for information about addresses and container conditions (volume, emptying frequency, price), the Danish Data Protection Authority must draw attention to the data protection regulation's definition of the concept of personal data, which follows from the regulation's article 4, no. 1.

It follows from Article 4, No. 1 of the Data Protection Regulation that personal data is any type of information about an identified or identifiable natural person who can be directly or indirectly identified, in particular by an identifier such as e.g. a name, an identification number, location data, an online identifier or one or more elements specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

In a situation such as the present one, the inspectorate must draw the municipality's attention to the fact that information about addresses and container conditions combined with other identifiers can relatively easily take the form of information that can be attributed to a person according to the regulation's definition in Article 4, No. 1.

In this context, the Danish Data Protection Authority must note that it is the opinion of the Danish Data Protection Authority that all personal data is worthy of protection, and that URL manipulation is a type of programming error source that is widely known and should be easily countered by the data controller. It cannot lead to a different result that the information is considered to be of a less sensitive nature, or weight is given to what the utility of the service is.

The Danish Data Protection Authority must therefore make it stricter that direct access to personal data is not given in any system via a URL, unless it has a complexity and length that cannot be easily guessed, deduced by machine or manipulated, this can - in order to further increase security - advantageous combined with multi-factor access control.

3.3 Summary

On the basis of the above, the Danish Data Protection Authority finds that there is a basis for expressing criticism that Herning Municipality's processing of personal data in the IT system: "Wasteweb" until 17 December 2021 has not taken place in accordance with the rules in Article 32, paragraph 1 of the Data Protection Regulation . 1.

Appendix: Legal basis

Extract from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).

Article 2, subsection 1. This regulation applies to processing of personal data that is carried out in whole or in part by means of automatic data processing, and to other non-automatic processing of personal data that is or will be contained in a register.

Article 4. In this regulation is understood by:

"personal data": any type of information about an identified or identifiable natural person ("the data subject"); identifiable natural person means a natural person who can be directly or indirectly identified, in particular by an identifier such as a name, an identification number, location data, an online identifier or one or more elements specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person

"processing": any activity or series of activities — with or without the use of automatic processing — to which personal data or a collection of personal data is made the subject, e.g. collection, registration, organization, systematization, storage, adaptation or modification, retrieval, search, use, disclosure by transmission, dissemination or any other form of transfer, compilation or combination, restriction, deletion or destruction

[…]

"data controller": a natural or legal person, a public authority, an institution or another body which, alone or together with others, decides for which purposes and with which aids the processing of personal data may be carried out; if the purposes and means of such processing are laid down in EU law or the national law of the Member States, the data controller or the specific criteria for appointing this may be laid down in the EU law or the national law of the Member States

Article 32. Taking into account the current technical level, the implementation costs and the nature, extent, context and purpose of the processing in question, as well as the risks of varying probability and seriousness to the rights and freedoms of

natural persons, the data controller and the data processor implement appropriate technical and organizational measures to ensure a security level that fits these risks, including as applicable:

pseudonymisation and encryption of personal data

ability to ensure ongoing confidentiality, integrity, availability and robustness of processing systems and services

ability to promptly restore the availability of and access to personal data in the event of a physical or technical incident

a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security.

PCS. 2. When assessing which level of security is appropriate, account is taken in particular of the risks posed by processing, in particular in the case of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or on otherwise treated.

PCS. 3. Compliance with an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element to demonstrate compliance with the requirements of this Article's paragraph. 1.

PCS. 4. The data controller and the data processor take steps to ensure that any natural person who performs work for the data controller or the data processor and who gets access to personal data only processes this on the instructions of the data controller, unless processing is required according to EU- court or the national law of the Member States.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).