ID validation in connection with requests for the exercise of data subjects' rights

Date: 25-10-2019

Decision

Private companies

A citizen complained that a company asked him to submit, for example, a passport or driving license before it would take a position on his request for deletion. The Danish Data Protection Agency found that the general procedure for ID validation was not in accordance with the rules, as the data controller has a duty to make a concrete assessment of whether there is reasonable doubt about the identity of the natural person.

Journal number: 2018-7320-0166

Summary

The Danish Data Protection Agency has made a decision in a case where a British citizen complained that Pandora A / S had asked him to submit identification in the form of a passport, driving license or a national identity card before Pandora would take a position on his request for deletion.

Pandora stated that, for security reasons, the company had established a general procedure for submitting credentials in connection with requests for the exercise of data subjects' rights.

The Data Protection Authority found that Pandora's general procedure, according to which, without exception, ID validation was required in connection with the processing of requests for the exercise of data subjects' rights, was not in accordance with the Data Protection Regulation.

The Danish Data Protection Agency emphasized, among other things, that the data controller has a duty to make a concrete assessment of whether there is reasonable doubt about the identity of the natural person, in connection with receiving requests for the exercise of data subjects' rights.

The case is the first case in which the Danish Data Protection Agency has made a decision as the leading supervisory authority under the “one-stop shop mechanism” in connection with cross-border processing of personal data.

Decision

The Danish Data Protection Agency hereby returns to the case, whereupon on 30 May 2018 it complained to The Information Commissioner's Office (ICO) that Pandora A / S (hereinafter Pandora) had refused to delete his personal information in

Pandora's systems / databases. In accordance with Article 56 of the Data Protection Regulation [1], the Data Protection Authority has been designated as the lead supervisory authority in the case.

Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Pandora's processing of personal data has not taken place in accordance with the rules in Article 12 (1) of the Data Protection Regulation. 6, and Article 5, para. 1, letter c.

The Danish Data Protection Agency also finds grounds for ordering Pandora to take a position on and against complaints to decide whether the conditions for deletion pursuant to Article 17 of the Data Protection Regulation are met and, if applicable, to delete the personal data processed on complaints. . The decision must be made as soon as possible and no later than two weeks from today's date. The injunction is granted pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter c.

The Danish Data Protection Agency draws attention to the fact that according to the Data Protection Act [2], section 41, subsection 2, no. 5, it is a criminal offense to fail to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Regulation. 2, letter c.

Pandora is asked to notify the supervisor when a decision has been made.

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

2. Case presentation

It appears from the case that on 23 May 2018, complainants contacted Pandora via email and requested to be deleted from the company's database.

In an email dated 29 May 2018, Pandora requested complaints to submit its request for deletion via the company's online form. Complainants then filled out the online form the same day, but due to technical issues, complainants took screenshots of the completed form and sent the photos of the completed form to Pandora via email.

On 30 May 2018, Pandora announced complaints that for the purpose of Pandora's processing of the request for deletion - in accordance with the requirements in the online form on the website - he had to submit identification in the form of e.g. passport, driving license or a national identity card in order for the company to be able to confirm his identity.

Complainants, however, did not want to send credentials to Pandora, so Pandora did not accede to plaintiffs' request for deletion, as Pandora, in its own view, could not reliably identify plaintiffs without the credentials.

2.1. Pandora's remarks

Pandora has stated that the registrant fills out the form on Pandora's website, which is sent encrypted to Pandora, after which it is stored in Pandora's internal systems and handled and answered by a designated employee. Since the data subject can enter any e-mail address in the form - even one that is not registered in Pandora's systems - the data subject will receive a confirmation email from Pandora immediately after submitting the request with a link that he / she must use to confirm the request.

Pandora has further stated that if the data subject enters an email address that is not registered in the company's systems or if there are other uncertainties in connection with the request, Pandora's customer service department will contact the data subject for clarification.

Once the request has been answered, Pandora confirms this to the data subject and the credentials attached to the form are deleted immediately after the request is processed. The identification is thus not stored for more than 30 days, unless the request procedure is extended pursuant to the Data Protection Regulation art. 12, para. 3.

Pandora has emphasized that the data subject's credentials are used solely for identity purposes and that Pandora never asks for credentials in connection with requests that only concern the data subject's desire to unsubscribe as a recipient of a Pandora newsletter (to which he or she has subscribed).

Pandora has stated that ID validation is an important part of Pandora's "DSR procedure" (abbreviation for data subject rights procedure). In Pandora's view, the company is required to verify the identity of the data subject before handling a DSR request from that person. Pandora has i.a. referred to recital 64 of the Data Protection Regulation, the Danish Data Protection Agency's guide on data subjects' rights section 2.6 and report no. 1565 on the Data Protection Regulation pkt. 4.2.2.4 (p. 269 ff.).

Pandora has stated that the company has approx. 9.7 million registered customers and that Pandora does not have a unique identifier (such as a customer or ID number) for each customer that can be used to validate the customer's identity. According to Pandora, any personal information that Pandora has registered in the company's systems (eg name, address, e-mail address and telephone number) is easy to search on e.g. social media and to some extent publicly available. It is Pandora's assessment that a procedure where Pandora does not ask for identification will involve a significant risk for Pandora's customers.

Pandora has stated that, in Pandora's view, the company's procedure fulfills the condition that the assessment of whether identification must be considered necessary must be assessed specifically in relation to the individual request. In this connection, Pandora has argued that because Pandora's relationship with the company's customers is primarily an online relationship where the company does not know the natural person behind the request, the specific assessment in each individual case will therefore be the same. In Pandora's view, therefore, there will either always be reasonable doubt and a general risk, or there will never be reasonable doubt or any general risk.

Given this complexity, Pandora initially conducted a risk assessment of the company's existing setup and, on this basis, established a procedure that, in Pandora's view, both meets the data subjects' rights in an easy and secure way, while Pandora complies with the company's obligations under the Data Protection Regulation. Article 12, paragraph 2 and 6, as well as the company's duty to ensure the identity of the data subjects and not unjustifiably disclose or delete personal data.

Pandora has stated that a more detailed assessment is not possible in the present case because there is no concrete information in the case that can be used as a valid basis for assuming that the data subject is the person he is pretending to be. be. Pandora argues that the request for identification in the specific case is necessary and overall proportionate.

Pandora has also referred to the fact that on 4 December 2018, the ICO ruled in a case materially identical to the present. In the present case, the ICO did not find grounds to criticize the fact that Pandora had asked a customer to submit identification in order to validate his identity prior to meeting the customer's request for deletion. The ICO assessed that the request for identification was proportionate.

2.2. Complainant's remarks

Complainants have generally stated that he did not wish to supplement Pandora with additional personal information in order to have the request for deletion granted. Complainants also allege that Pandora could have contacted him by email or phone to confirm his identity.

Justification for the Danish Data Protection Agency's decision

It follows from Article 12 (1) of the Data Protection Regulation 2, that the data controller must facilitate the exercise of the data subject's rights in accordance with e.g. Article 17 on deletion.

Pursuant to Article 12 (1) of the Data Protection Regulation 6, a data controller may, if there is reasonable doubt about the identity of the natural person making a request for e.g. delete, request any additional information necessary to verify the

identity of the data subject.

Furthermore, it follows from the data protection regulation's principles for the processing of personal data that personal data i.a. shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are dealt with, in accordance with Article 5 (2). 1, letter c.

The Danish Data Protection Agency also refers to the Article 29 Working Party's guidelines on the right to data portability WP242 rev.01 [3], page 14 et seq. the following appears:

"There are no prescribed requirements in the Data Protection Regulation on how the data subject can be authenticated. (…) In addition, Article 12 (2) provides: 6, that if a data controller has reasonable grounds for suspecting the identity of a data subject, he or she may request additional information in order to confirm the data subject's identity. (…) If information and data collected online are linked to pseudonyms or unique identifiers, data controllers may perform appropriate procedures enabling a natural person to request data portability and receive information relating to him or her. In all cases, the data controller must establish a procedure for verifying authenticity in order to be able to establish with certainty the identity of the data subject requesting his personal data or, more generally, exercising the rights conferred by the Data Protection Regulation.

These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or obtaining consent for processing. As a result, the personal data used to register the natural person concerned during the processing may also be used as evidence to authenticate the data subject for portability purposes.

In these cases, a request for proof of the legal identity of the data subjects may be required, while verification may be relevant to assess the link between the information and the natural person concerned, as such a link does not relate to the official or legal identity. In essence, the possibility for the data controller to request additional information to identify a person's identity may not lead to excessive claims and to the collection of personal data that are not relevant or necessary to strengthen the link between the natural person and the personal data requested. about.

In many cases, such verification procedures have already been initiated. For example, often usernames and passwords to give individuals access to data on email accounts, social networking accounts and accounts of various other services where individuals choose to use some of these without revealing their full name and identity. "

The Danish Data Protection Agency assumes that Pandora always requests identification in connection with a request from a data subject who wishes to make use of his rights.

Following an examination of the case, the Danish Data Protection Agency's assessment is that Pandora's general procedure, according to which ID validation is required without exception in connection with processing requests for the exercise of data subjects' rights, is not in accordance with Article 12 (1) of the Data Protection Regulation. 6, and Article 5, para. 1, letter c.

The Danish Data Protection Agency has emphasized that Article 12 (1) of the Data Protection Regulation 6, implies that the data controller has a duty to make a concrete assessment of whether there is reasonable doubt about the identity of the natural person, in connection with the individual request for the exercise of the data subject's rights. In this connection, the Danish Data Protection Agency finds that the fact that there is an online customer relationship cannot mean that there will always be reasonable doubt about the identity of the natural person.

The Danish Data Protection Agency has also emphasized that a request for additional information in order to identify the natural person must be proportionate, cf. Article 5 (1). 1, letter c, and the data controller must therefore not demand more information than is necessary to be able to identify the natural person. The Danish Data Protection Agency finds that it is not in accordance with Article 12 (1). 2, that Pandora has organized a procedure whereby the data subject must provide more information than was originally collected in order to have a request for the exercise of data subjects' rights processed.

The fact that Pandora has arranged its systems in such a way that e.g. If unique identifiers are not linked to the data subjects, the Danish Data Protection Agency's assessment cannot lead to a justification for Pandora in all cases requiring the data subject to identify himself in order to be able to exercise his rights under the Regulation. In the opinion of the Danish Data Protection Agency, Pandora's general procedure for ID validation goes beyond what is required and unnecessarily complicates the data subject's ability to exercise his rights.

In the light of the above, the Danish Data Protection Agency thus finds grounds for expressing criticism that Pandora's processing of personal data has not taken place in accordance with the rules in Article 12 (1) of the Data Protection Regulation. 6, and Article 5, para. 1, letter c.

The Danish Data Protection Agency also finds grounds for ordering Pandora to take a position on and against complaints to decide whether the conditions for deletion pursuant to Article 17 of the Data Protection Regulation are met and, if necessary, to delete the personal data processed on complaints. .

The Danish Data Protection Agency notes that in connection with its handling of complaints, the Authority will always make a concrete assessment of the circumstances. In the opinion of the Danish Data Protection Agency, a reference to a decision

made in another European country may not necessarily lead to the Authority making a similar decision.

[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] At its first meeting on 25 May 2018, the European Data Protection Board confirmed that this is also an expression of the Council's position.