DATATILSYNET

Pandora A/S
Havneholmen 17-19
1561 Copenhagen V
Denmark

Sent with Digital Post

25 October 2019

J.No. 2018-7320-0166
Doc.no. 137612
Caseworker
[redacted]

Complaint about processing of personal data

The Danish Data Protection Agency
Borgergade 28, 5.
1300 Copenhagen
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. [redacted]

The Danish Data Protection Agency returns to the case where, on the 30th of May 2018, [redacted] (hereinafter: the complainant) complained to the Information Commissioner's Office (ICO) that Pandora A/S (hereinafter: Pandora) has refused to delete his personal data in Pandora's systems/databases. In line with Article 56 of the General Data Protection Regulation[1], the Danish Data Protection Agency has been designated as the leading supervisory authority of the case.

1. Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds to **criticize** that the processing of personal data by Pandora has not been done in accordance with the rules of Article 12(6) and Article 5(1)(c) of the General Data Protection Regulation.

The Data Protection Agency also finds basis to **order** Pandora in the complainant's case to make a decision whether the conditions for erasure under Article 17 of the General Data Protection Regulation have been met and, if so, to delete the personal data processed about complainant. The decision shall be taken as soon as possible and **no later than two weeks from the date of this letter**. The order is granted pursuant to Article 58(2)(c) of the General Data Protection Regulation.

The Data Protection Agency draws attention to the fact that, pursuant to Paragraph 41(2)(5) of the Data Protection Act[2], failure to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58(2)(c) of the Regulation is punishable.

Pandora is requested to notify the agency when a decision has been made.

The details of the case and the reasons for the decision of the Danish Data Protection Agency are set out below.

[1] Regulation (EU) 2016/679 Of The European Parliament And OF The Council of 27 April 2016 on the protection of natural persons 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 natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

2. Statement of facts

On the 23th of May 2018 the complainant contacted Pandora by e-mail and requested to be deleted from the company's database.

In an e-mail of the 29th of May 2018, Pandora requested that the complainant submit his request to be deleted via the company's online form.

The complainant then completed the online form on the same day, but due to technical problems, the complainant took some screenshots of the completed form and sent the images of the completed form to Pandora via e-mail.

On the 30th of May 2018 Pandora informed the complainant that in order to process his request for deletion he had to submit proof of identification in the form of, for example, passport, driving license or national identity card, in order to confirm his identity, in accordance with the requirements of the online form on the website.

However, the complainant did not wish to send proof of identity to Pandora. Therefore, the complainant's request for deletion was not granted since, in Pandora's opinion; Pandora was not able to identify the complainant with certainty without proper identification.

2.1. Pandora's remarks

Pandora has stated that the data subject fills in the form on the Pandora homepage, which is sent encrypted to Pandora, after which it is stored in Pandora's internal systems and is handled and answered by a designated employee. As the data subject can enter any e-mail address in the form, including one which is not registered in Pandora's systems, the data subject will after submitting his/her request immediately receive a confirmation e-mail from Pandora with a link to be used to confirm the request.

Pandora has also stated that if the data subject enters an e-mail address that is not registered in the company's systems, or there are other uncertainties regarding the request, Pandora's customer service department contacts the data subject for clarification.

Once the request has been answered, Pandora will confirm this to the data subject and the proof of identification attached to the form will be deleted immediately after the application has been handled. The proof of identification will not be stored more than 30 days, unless the request is extended pursuant to Article 12(3).

Pandora has stressed that the proof of identity of the data subject is exclusively used for identity purposes, and that Pandora will never ask for identification in connection with requests that relate only to the data subject's wish to be deregistered as recipient of a Pandora newsletter (which he/she has registered for).

Pandora has indicated that ID validation is an important part of Pandora's DSR procedure (data subject rights procedure). In the case of Pandora, the company is obliged to verify the identity of the data subject before a DSR request is handled. In particular, Pandora has referred to recital 64 of the General Data Protection Regulation, the Danish Data Protection Agency's guidance on data subjects' rights section 2.6 and report No 1565 on point 4.2.2.4 of the Data Protection Regulation.

Pandora has stated that it has around 9,7 million registered customers and Pandora does not have a unique identifier (e.g. customer or ID number) for each customer that can be used to validate the customer's identity. The personal data, if any, recorded by Pandora in the company's systems (e.g. name, address, e-mail address, phone number), according to Pandora

are easy to look up on social media and the information is, to some extent, publicly available. It is Pandora's view that a procedure in which Pandora does not request proof of identity would entail a significant risk for Pandora's customers.

Pandora states that, in the opinion of Pandora, the company's procedure fulfils the condition that the assessment of whether proof of identity is to be considered necessary must be assessed on a case-by-case basis in relation to the individual request. Pandora argues in this respect that because the relationship of Pandora to its customers is primarily an online environment in which the company does not know the natural person behind the request, the individual assessment will be the same in each case. Therefore, in the opinion of Pandora, there will either always be a reasonable doubt and a general risk, or there will be no reasonable doubt or a general risk.

In view of this complexity, Pandora initially carried out a risk assessment of the existing set up of the company and established on this basis a procedure which, in the opinion of Pandora, meets both the rights of the data subjects in an easy and secure manner, while Pandora observed the undertaking's obligations under the General Data Protection Regulation including the requirements set out in Article 12(2) and (6), as well as the obligation for the company to guarantee the data subjects' identity and not to unjustifiably provide or delete any personal data.

Pandora has argued that, in the present case, a specific assessment is not possible because there is no concrete information in the case that can be used as valid evidence to assume that the data subject is the person he claims to be. Pandora claims that, in the specific case, the request for proof of identity is necessary and proportionate.

In addition, Pandora has referred to the fact that the ICO on the 4th of December 2018 made a decision in a case that is by substance identical to the present one. The ICO did not find, in that case, grounds for criticizing the fact that Pandora had requested a customer to send proof of identity in order to validate his/her identity prior to processing the request for deletion by the customer. The ICO considered the request for identification to be proportionate.

2.2. The complainant's remarks

The complainant has generally stated that he did not want to give Pandora further personal data in order to have his deletion request processed. The complainant also claims that Pandora could have contacted him by e-mail or telephone in order to confirm his identity.

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

It follows from Article 12(2) of the General Data Protection Regulation that the controller should facilitate the exercise of the data subject's rights pursuant, inter alia, to Article 17 on erasure.

Under Article 12(6) of the General Data Protection Regulation, a controller may, if there is reasonable doubt as to the identity of the natural person making a request, demand additional information necessary to confirm the identity of the data subject.

It also follows from the principles relating to processing of personal data provided by the General Data Protection Regulation that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in accordance with Article 5(1)(c).

The Danish Data Protection Agency furthermore refers to the Article 29 Working Party guidelines on the right to "data portability" (wp242rev.01[3]), page 13, which states that:

> "There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. (…) Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject's identity. (…) Where information and data collected online is linked to pseudonyms or unique identifiers, data controllers can implement appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.
>
> These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing. As a consequence, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for portability purposes.
>
> While in these cases, the data subjects' prior identification may require a request for proof of their legal identity, such verification may not be relevant to assess the link between the data and the individual concerned, since such a link is not related with the official or legal identity. In essence, the ability for the data controller to request additional information to assess one's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.
>
> In many cases, such authentication procedures are already in place. For example, usernames and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity."

The Danish Data Protection Agency assumes that Pandora always requests proof of identity from a data subject when a data subject wishes to exercise his/hers rights.

On the basis of a review of the case, the Danish Data Protection Agency finds that Pandora's general procedure, under which ID validation is required without exception when processing a requests to exercise the rights of the data subjects, is not in conformity with Article 12(6) and Article 5(1)(c) of the General Data Protection Regulation.

The Danish Data Protection Agency has attached importance to the fact that Article 12(6) of the General Data Protection Regulation requires the controller to carry out a specific assessment as to whether or not there are reasonable doubts as to the identity of the individual in relation to the individual application for the exercise of the rights of the data subject. The Danish Data Protection Agency considers in this context that the fact that there it is an online customer relationship does not mean that there will always be reasonable doubts about the identity of the natural person.

[3] During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines, including wp242rev.01.

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

The fact that Pandora has failed to set up its systems in such a way that, for example, unique identifiers are attached to data subjects, cannot justify that Pandora requires, in all cases, that the data subject provides proof of identification in order to be able to exercise his/hers rights under the regulation. In the view of the Danish Data Protection Agency, Pandora's overall procedure for ID validation goes beyond what is required and makes it unnecessarily burdensome for the data subject to exercise his/her rights.

On the basis of the above, the Danish Data Protection Agency **criticizes** that the processing of personal data by Pandora has not been done in accordance with the rules of Article 12(6) and Article 5(1)(c) of the General Data Protection Regulation.

The Data Protection Agency also finds basis to **order** Pandora in the complainant's case to make a decision whether the conditions for erasure under Article 17 of the General Data Protection Regulation have been met and, if so, to delete the personal data processed about complainant.

The Danish Data Protection Agency notes that the agency in its handling of complaints will always carry out a specific assessment of the facts. In the view of the agency, a reference to a decision taken in another European country cannot necessarily lead to a corresponding decision being taken by the agency.

4. Final remarks

The Danish Data Protection awaits notification from Pandora. The notification must be received within two weeks of today's date.

The Data Protection Agency has informed the ICO of the decision in order for the ICO to pass on the decision to the complainant.

It should be noted that the Data Protection Agency expects to publish this decision on the agencies website.

Kind regards

[redacted]

Appendix: Legal basis

Appendix: Legal Basis

Extracts from Regulation (EU) 2016/679 Of The European Parliament And OF The Council of 27 April 2016 on the protection of natural persons 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).

Article 5. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that accurate, having regard to the purposes for which they are processed, are erased or rectified without delay 'accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 12. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the

data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.