[redacted]

Sent by Digital Post

21 May 2024

J.No. 2023-7333-0001
Doc.no. 588967
Caseworker
[redacted]

Final decision pursuant to Article 60(8) of the GDPR

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

1. The Danish Data Protection Agency (hereinafter 'the Danish DPA') hereby returns to the case where, on 1 March 2023, you lodged a complaint with the Danish DPA against Zalando SE ('Zalando') concerning erasure of your account and related information.

Due to a new period of journaling, the case has now the following case ref.: 2023-7333-0001 (former case ref.: 2023-7333-0076).

The Danish DPA has considered that the case involves cross-border processing of personal data, which has meant that the case has been handled in cooperation with the supervisory authorities of the other EU Member States.

The Berlin Commissioner for Data Protection and Freedom of Information (hereinafter 'the Berlin DPA') has been designated as lead supervisory authority in the case in accordance with Article 56 of the GDPR[1], as Zalando's main business is established in Berlin. The Berlin DPA has therefore dealt with the matter and examined the circumstances in more detail. The case has been handled in accordance with the procedure laid down in Article 60 of the GDPR.

2. On the basis of the Berlin DPA's investigation of the case, the Danish DPA considers that Zalando's processing of personal data has been carried out in accordance with the rules of the GDPR.

The Danish DPA has emphasised the statement from the Berlin DPA, which is set out below:

> "The complaint points out the fact that Zalando SE has not deleted the complainant's customer account, contrary to legal requirements. Based on the information provided and the attached e-mail correspondence with customer service, the facts are as follows:
>
> Unknown third parties were able to gain access to the complainant's customer account and placed an order. The complainant reported this to Zalando. As a result, the customer account was blocked on February 2, 2023, so that the complainant and other persons could no longer access it. The complainant then asked

[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.

Zalando to erase his/her personal data. Zalando informed the complainant that the customer account had been blocked, but that his/her personal data could only be erased 100 days after his/her last order. The background to this is that Zalando contractually guarantees a 100-day right of return. Zalando has assured the complainant of erasure by May 22, 2023.

The complainant is of the opinion that Zalando should have deleted the customer account immediately, as the complainant would have revoked his/her consent regarding the processing of his/her data.

Without prejudice to a comprehensive review, the Berlin DPA hereby informs the complainant of the following:

Based on the complainant's description of the facts, the Berlin DPA cannot identify any infringement of data protection regulations.

First of all, the Berlin DPA cannot identify any infringement of Art. 32 GDPR, i.e. the security of processing, at Zalando.

Insofar as only individual customer accounts were accessed by unauthorized third parties, it is reasonable to suspect that this was done through so-called "credential stuffing". Credential stuffing" refers to attacks in which access data that has become public through other data breaches is tried out on other services. This can involve specific combinations of e-mail addresses/usernames and passwords from a common source, but also from different sources.

Such attacks are difficult for companies to prevent. If the login to the customer's account is done using the actual credentials, it is usually very difficult for companies to detect whether the login is done by the true account holder or an unauthorized person. Contrary to common expectations, passwords do not have to be bad or weak in this case; even passwords that are considered strong can be affected if they were exposed in a past data breach. The remedy against this kind of attack is, in particular, the consistent avoidance of password reuse. It is recommended to use a separate password for each service. For usability, we recommend the use of a secure password manager.

Zalando has also blocked the complainant's customer account for security reasons. This is a suitable technical and organizational measure to protect the customer account from further access by third parties.

With regard to the erasure of the account, the Berlin DPA is also unable to identify any infringement of data protection regulations on the basis of the complainant's description of the facts.

Pursuant to Art. 17(1) of the GDPR, the data subject has the right, if one of the reasons listed is available for it, to demand that the controller delete personal data relating to him or her without undue delay. In addition, if one of the grounds of Art. 17(1) GDPR is available for, there is an obligation for the controller to erase without undue delay, irrespective of a request by the data subject.

The Berlin DPA would first like to point out that a revocation of consent does not necessarily mean that personal data must be deleted. Pursuant to Art. 17(1)(b) GDPR, personal data must be deleted in the event of a revocation of consent if

the specific processing is based on consent (Art. 6(1)(a) or Art. 9(2)(a) GDPR) and there is no other legal basis for the processing.

In the present case, Zalando bases the fact that the customer account was initially only blocked, but not yet deleted, on the fact that Zalando contractually guarantees a 100-day right of return and that the last order from the complainant's customer account was less than 100 days ago. The fact that Zalando grants the 100-day right of return also results from point 8 of the general terms and conditions of Zalando, which can be found on the website and which the Berlin DPA has viewed on 23 May and 23 November 2023. Zalando should thus base the further storage on the processing of a (purchase) contract (Art. 6(1)(b) GDPR), to the extent that the data are necessary for this purpose, which is to be verified by the controller. Insofar as there is a misuse of identity and you may not have become a contractual partner of Zalando with regard to the order in question, Zalando may be able to base further storage, if not on Art. 6(1)(b) GDPR, at least on Art. 6(1)(f) GDPR until the expiry of the 100-day return period. Art. 6(1)(f) GDPR permits data processing if it is necessary to protect the legitimate interests of the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject override these. However, here too, controllers must limit storage to what is necessary to achieve the purpose. In the present case, Zalando is likely to have a legitimate interest - also in the case of an alleged identity theft - in retaining the data related to the order until the expiry of the return period in order to be able to respond to a theoretical possible assertion of the right of return. Due to the fact that the customer account has already been blocked and the limited period of time until erasure (100 days after the last order, according to Zalando on May 22, 2023), the complainant's interest in immediate erasure should not prevail.

Based on this assessment, the Berlin DPA assumes that in the present case no GDPR violation has actually occurred.

We thank the complainant for informing us of the facts above. As far as the complaint is concerned, the Berlin DPA considers the matter closed and rejects this complaint under Art. 60(8) GDPR."

The Danish DPA adopts the decision pursuant to Article 60(8) of the GDPR.

3. Concluding remarks

The Danish DPA considers the case closed and does not take any further action.

The decisions of the Danish DPA cannot be brought before any other administrative authority, cf. Section 30 of the Danish Data Protection Act[2]. However, the decisions of the Danish DPA can be brought before the Danish courts, cf. Section 63 of the Danish Constitution.

The Danish DPA publishes decisions on an ongoing basis on the Danish DPA's website in pseudonymized form. If this decision is published, this will therefore be done in such a way for individuals not to be immediate identified.

Kind regards

[2] Act No. 502 of 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). A translated version is available here. Only the Danish version of the text has legal validity.

[redacted]