Swedish Authority for Privacy Protection

Boozt Fashion AB
Hyllie Boulevard 35
215 37 Malmö

Our ref.:
DI-2020-10544, IMI no. 115751

Date:
2021-06-17

Supervision under the GDPR – Boozt Fashion AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that the investigation in the matter does not show that Boozt Fashion ABhas processed the complainant's personal data in violation of the GDPR[1].

The case is closed.

Report on the supervisory matter

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Boozt Fashion AB (the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Denmark) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The *complainant* states that the company has provided the complainant's e-mail address to third parties (Facebook) for the purpose of sending direct marketing to the complainant without having a legal basis for it. In December 2018, the complainant requested access pursuant to Article 15 of the GDPR from Facebook, which revealed that the company has disclosed the complainant's personal data to Facebook.

Boozt Fashion AB has mainly stated the following. The company is not the controller for the processing that the complaint concerns since the company's processing of the complainant's e-mail address took place before the application of the GDPR. The complainant's e-mail address was collected in 2016 in connection with a purchase from the complainant. In 2017, the complainant's email address was sent to Facebook in order to be able to target marketing using Facebook's custom audience function. This process was carried out in accordance with the current legislation. In spring 2018, before the introduction of the GDPR on 25 May 2018, Facebook changed its terms for the custom audience function. The company did not accept the terms and conditions and Facebook set the personal data that the company has transferred to Facebook in

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

[1] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (GDPR).

quarantine while waiting for the company to accept the new terms. The company did not give Facebook any instructions to quarantine the personal data, but the initiative came from Facebook. During this period, the Company did not have access to or the possibility to use, modify or delete the personal data. The company approved Facebook's new terms in January 2019 and the quarantine personal data was then unlocked by Facebook, after which the company deleted the complainant's information. The company believes that the reason for the complainant's excerpt at Facebook in December 2018 revealed that the company had transferred the complainant's personal data to Facebook because that information remained from the transfer in 2017.

The company disputes that any processing of the complainant's personal data for direct marketing purposes has taken place, neither during the time when the personal data was quarantined by Facebook or during the time the GDPR has been applicable. According to the company, the company is only the controller for the transfer of the complainant's personal data to Facebook and for any direct marketing that has taken place before the personal data was quarantined, i.e. before the GDPR began to apply. Furthermore, the company has stated that during the period of the GDPR, the company has only processed the data subjects' personal data for direct marketing with their prior consent.

The investigation has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, France, Italy, Norway, Germany, Spain, Austria, Poland and Finland.

Justification of the decision

The assessment of the Authority for Privacy Protection (IMY)

Processing of personal data
According to Article 4(2) of the GDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Examples thereof is collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller
The controller, according to Article 4(7) of the GDPR, is the person who alone or together with others determines the purposes and means for the processing of personal data. If two or more controllers jointly determine the purposes and means of processing, they are joint controllers. According to Article 26, they are then obliged to establish their respective responsibilities in order to fulfil their obligations under the GDPR under an open form, through mutual arrangements. This means that the arrangement between the responsible parties must contain specific information about how the obligations under the regulation are to be fulfilled in practice. If there is no clarity as to how the obligations should be fulfilled, especially with regard to the rights of data subjects, both parties may be deemed to be acting in violation of Article 26(1) of the GDPR.

The purpose of these rules is to ensure that the responsibility for compliance with data protection rules is clearly distributed in cases where several actors participate, to avoid the reduction of the protection of personal data and lead to loopholes where certain obligations are not met by any of the parties involved in the processing.[2]

The Court of Justice of the European Union has stated in the case *Wirtschaftsakademie* that a common responsibility does not necessarily mean that the various actors involved in the processing of personal data have an equal responsibility.[3] The actors can be involved in different stages of treatment and to different extents. The responsibility for each of them shall be assessed taking into account all relevant circumstances in the case.

In the *Fashion ID* case, the Court of Justice of the European Union concluded that a website operator using plugins on its website that enables website visitors' personal data to be transferred to a social media provider may be considered to be joint data controller with the social media provider.[4] The court stated that the responsibility is limited to the parts of the processing chain for which the website operator actually determines the purposes and means for. In this case, the European Court of Justice considered that the website operator was only involved in determining the purposes and funds for collection and disclosure by transferring personal data about its visitors to the social media provider. The website operator was not considered responsible for the later measures carried out by the social media provider after the data had been disclosed to the latter, as the website operator was not involved in determining the purposes and means of subsequent processing.[5]

The company has stated that it has been the controller for the collection and transfer of the complainant's personal data to Facebook before quarantining the data. The question is therefore whether the company has been jointly controller during the time the personal data was quarantined, i.e. from spring 2018 (before the introduction of the GDPR and when Boozt did not approve Facebook's conditional changes) until January 2019 (when the personal data was erased).

The company transferred the complainant's email address to Facebook for the purpose of direct marketing to the complainant. From the moment the personal data was locked by Facebook, no direct marketing has been made to the complainant. Since the company did not approve Facebook's conditional amendments, it could not continue to process the personal data for the purpose it was transferred to Facebook. The company also did not instruct Facebook to store the personal data in quarantine. In the circumstances, the purpose of the processing seems to have changed when Facebook unilaterally decided to quarantine the complainant's personal data. This indicates that Facebook alone determined the purpose and means of processing and that Facebook has been solely responsible for the continued processing (storage).

When it comes to assessing the distribution of responsibilities between a controller who collected and transferred personal data to a social media provider for the purpose of direct marketing and the social media provider, several factors may be relevant. For example, the ability to influence the processing on a practical level, as well as the actual knowledge (or the knowledge they should have had) of each of the joint

---

[2] European Data Protection Board's (EDPB) Guidelines 07/2020 on the concepts of controller and processor in the General Data Protection Regulation, paragraph 160.
[3] European Court of Justice ruling of 5 June 2018, Wirtschaftsakademie, case C-210/16, paragraph 43.
[4] The European Court of Justice's judgment of 29 July 2019, Fashion ID, case C-40/17, paragraph 85.
[5] Fashion ID, item 76.

controllers.[6] However, it is not required that each operator in a joint processing has actual access to the personal data concerned in order to be considered jointly responsible.[7]

In the present case, it has not been shown that the company had the opportunity to dispose of the data or affect the processing of the data while quarantined. Furthermore, the company has stated that it lacked knowledge of whether Facebook has directed direct marketing to the complainant while the personal data was locked.

In an overall assessment of the circumstances, IMY finds that the company cannot be regarded as a joint data controller while the personal data was locked by Facebook.

Conclusion

This supervision covers only the company's processing of the complainant's personal data in accordance with the GDPR.

The investigation has shown that the company's processing of the complainant's personal data has taken place before the application of the GDPR. From the time the complainant's personal data was quarantined by Facebook, which occurred before the application of the GDPR, the parties joint data controllership ceased resulting in that Boozt Fashion AB was no longer responsible for the continued processing of the complainant's personal data.

IMY therefore finds that the investigation in the case does not show that Boozt Fashion AB has processed the complainant's personal data in violation of the GDPR.

The case is closed.

This decision has been made by Head of Unit [redacted] after presentation by legal advisor [redacted]. The legal advisor [redacted] has also participated in the handling of the case.

Copy to
Counsel in the matter

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-06-16, no. DI-2020-10544. Only the Swedish version of the decision is deemed authentic.

---

[6] EDPB's guideline 8/2020 on targeted advertising to social media users, point 133.
[7] The European Court of Justice's judgment of 10 July 2018, Jehovah Todistajat, case C25/17-, paragraph 69.