Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-08-18, no. IMY-2022-86. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-86, IMI case no. 134934

Date of final decision:
2022-08-18

Date of translation:
2022-08-24

Final decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that the investigation has not shown that Klarna Bank AB has processed the complainant's personal data in breach of Article 32 or 33 of the General Data Protection Regulation (GDPR)[1] in the manner alleged in the complaint.

The case is closed.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations 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 (Norway) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, The Netherlands, Denmark, Finland, Italy, Spain and Austria.

The complaint

The complaint states the following. After an online purchase, the complainant chose to use Klarna's invoice options. A few days after the purchase was made, the complainant received several messages and calls from persons who were able to access the complainant's invoice. The complainant contacted Klarna's customer service who was unable to provide any information about the incident. As far as the complainant is aware, unauthorised persons have been able to access the

[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 he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

complainant's invoice by e-mail. The invoice contains the name of the complainant, however, the persons who received e-mails containing the complainant's invoice also had access to the complainant's address and telephone number, because they managed to contact the complainant.

What PUA has stated
Klarna Bank AB has mainly stated the following. Klarna is the data controller for the processing to which the complaint relates.

The company initiated their own investigation after having received calls to its customer service from several persons who incorrectly received the complainant's invoice in February 2019. The investigation found that Klarna did not unlawfully disclose the complainant's personal data. According to the company's investigation it is likely that unauthorised persons have logged in to the complainant's e-mail account and found the invoice from Klarna. The reason for this assumption is that the complainant's login details have been available on a Russian hacker forum. These unauthorised persons have then sent the invoice to other recipients and pretended to be Klarna. However, it is not Klarna who has been the sender of these messages. Since Klarna has not been the sender, it is not possible for Klarna to know exactly how this has been done, but one possibility is so-called e-mail spoofing.[2]

Klarna has not reported a personal data breach to IMY due to the incident because the disclosure of personal data has not been made from within its own organisation. However, in connection with the incident, Klarna contacted the complainant and provided the requested information and informed about the measures that could be taken to minimise the risk of further unauthorised disclosures of the data.

Justification of the decision

Applicable provisions, etc.

Article 4(1) of the GDPR defines the term 'personal data' as any information relating to an identified or identifiable natural person.

Article 4(2) states that "processing" means any operation or combination of operations concerning personal data or sets of personal data.

According to Article 4(7), the controller is a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Assessment of the Authority for Privacy Protection (IMY)

Klarna has stated that the company is not the data controller for the processing of personal data to which the complaint relates. Furthermore, Klarna states that it did not disclose the complainant's personal data to any unauthorised person and argues that, according to its own investigation, an explanation for the incident may be that someone has accessed the complainant's e-mail account due to the fact that the complainant's login information was available on the internet.

[2] Email spoofing is the creation of email messages with a forged sender address.

IMY notes that there has been no reason to question what the company has stated. Against this background, IMY finds that the investigation at hand has not shown that Klarna Bank AB failed to comply with the General Data Protection Regulation in the manner alleged in the complaint.

The case is closed.

This decision has been made by the specially appointed decision-maker [redacted] after presentation by legal advisor [redacted].