Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2024-09-20, no. DI-2021-1686. Only the Swedish version of is authentic. The English version is for information purposes only.

Klarna Bank AB
fd.regulatory.gateway@klarna.com

Swedish reference number:
DI-2021-1686

IMI case register:
91812

Date of draft decision:
2024-09-20

Date of translation:
2024-09-20

Final decision pursuant to Article 60 under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Klarna Bank AB has processed personal data in breach of Article 32 of the General Data Protection Regulation.[1] This has been done by Klarna Bank AB sending privacy-sensitive personal data about the complainant by e-mail without using a sufficiently secure encryption solution. Klarna Bank AB has therefore not taken appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing.

The Swedish Authority for Privacy Protection issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 32 GDPR.

Presentation of the supervisory case

Handling of the case

The Swedish Data Protection Authority (IMY) has received a complaint against Klarna Bank AB (hereinafter Klarna) in accordance with the provisions on the competence of the lead supervisory authority in Article 56 of the General Data Protection Regulation (GDPR). The complaint was lodged with the German data protection authority Rhineland-Palatinate on 21 November 2018.

The complainant has essentially stated the following. He opened an online account with Klarna in November 2018. The complainant subsequently received unencrypted e-mails concerning his bank account containing the bank account holder's (the complainant's) name, figures which the complainant perceived as his bank account number, the amount of the investment, the current interest rate and the commitment period of the investment. The complainant does not want his personal data or details of his bank account to be accessible to unauthorised persons and has informed Klarna that the relevant information has been sent unencrypted by e-mail. Klarna has informed the complainant that this was the usual way of communication. In response to the complaint, IMY has initiated supervision in order to investigate whether Klarna

[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).

Postal adress:
Box 8114
104 20 Stockholm

Webbsite:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+4608-657 61 00

has ensured an appropriate level of security in accordance with Article 32 of the GDPR for the processing in question.

The supervision at IMY has been handled through written procedure. Klarna has had the opportunity to comment on IMY's draft decision. In view of the cross-border nature of the processing, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. Relevant supervisory authorities have been the data protection authorities in Denmark, Finland, Norway, Poland, Germany, France, Austria and Italy.

What Klarna states

Liability of the controller
Klarna has essentially stated the following. The complainant has held a savings account with Klarna in Germany since November 2018. Klarna's savings accounts in Germany are administered by the German bank Süd-West-Kreditbank Finanzierung GmbH ("SWK"), on behalf of Klarna. SWK also offers and manages this type of savings account for its own customers (consumers), as well as on behalf of other banks. Klarna is the controller and SWK is Klarna's processor regarding the processing of the e-mail correspondence to the complainant.

Types of personal data to which the processing in question relates
Klarna has, through its processor SWK, sent information by e-mail containing the complainant's name, investment amount, interest of the savings account, commitment period of the investment and the Klarna reference number to the complainant by e-mail in connection with the opening of the savings account.

The complainant's bank account number was not included in the e-mail correspondence in question. The combination of numbers that the complainant perceives as his bank account number is a reference number to Klarna. The complainant specifies the Klarna reference number when making deposits at SWK in order for the money to be allocated correctly.

What technical security measures have been applied in the processing in question
SWK operates in accordance with German banking regulations, and its data protection management is third-party certified by TÜV Rheinland, which is a standard certification in Germany.

The personal data transferred from SWK to the complainant was sent encrypted. Klarna's server has at the time of transfer had the opportunistic setting of the encryption protocol TLS (Transport Layer Security), version 1.2, which provides confidentiality, authentication and privacy protection. Through the use of the opportunistic TLS server, Klarna's server has automatically negotiated a TLS level that both their server and the recipient's server support (if any). By the negotiation, protected links are created between the sender and the recipient of the email, ensuring the secure transmission of the data.

TLS is a globally implemented and accepted standard for sending information between terminal equipment over the internet. Most email providers, such as Gmail, Yahoo, GMX, Outlook from Microsoft, iCloud from Apple, AOL and ProtonMail, as well as the provider used by the complainant, support and use TLS. In Germany, where SWK provides its services, neither Klarna nor SWK have identified any email provider that

does not support TLS 1.2. Thus, there has been no indication that emails were sent without TLS. Once the email has reached the recipient, it is then subject to the security measures of the recipient's email provider.

Requirements for appropriate technical security measures at the time of the complaint
The personal data processing that is relevant in this case took place in November 2018. The technical security measures used in the present case must therefore be assessed in accordance with the professional practice at the time of the processing in question. At the time of the complaint, TLS version 1.2 was considered a secure means of transmitting personal data by e-mail. At that time, there were also no uniform guidelines from German authorities on security measures for this type of processing or personal data.

Furthermore, the savings account in question does not constitute a ‘payment account’. It is only possible to make deposits into, or payments from, the savings account in question to a specific external transaction account specified by the customer, which is linked to the savings account. The savings account is therefore not covered by Directive 2015/2366 (“PSD2”), or the European Banking Authority’s recommended security measures for payment accounts.

The personal data covered by the processing at issue cannot be used to enable payments to be made to a bank account other than the bank account linked to the savings account by the complainant. Moreover, the use of the data at issue could not have enabled any other type of fraud to be committed against the complainant.

In light of the categories of personal data sent, and the technical security measures used, Klarna and SWK consider that the emailing processing complied with the requirements for technical security measures in Article 32 GDPR.

Klarna's new solution for managing e-mail messages
Klarna has stated that, in the period following the complaint, SWK has continuously strengthened the technical security measures it uses when sending e-mails by launching a new communication solution for e-mails to its customers.

Motivation for the decision

Applicable provisions

The controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. When assessing the appropriate technical and organisational measures, the controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (Article 32(1) GDPR).

Pursuant to Article 32(1) of the GDPR, appropriate measures may include, inter alia:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (Article 32(2) GDPR).

In accordance with Chapter 1, Section 10 of the Banking and Financing Business Act (2004:297), there is an obligation of confidentiality and secrecy for the circumstances of individuals with credit institutions.

An individual's relationship with a credit institution means, inter alia, an ongoing customer relationship between a natural person and a bank.[2]

Assessment

Klarna has stated that it is the controller for the processing described in the case. IMY finds no reason to question that Klarna is the controller for the processing included in the current e-mail correspondence.

Personal data shall be processed in a way that ensures an appropriate security level of the personal data based, inter alia, on their sensitivity. Information about an individual's financial situation does not constitute sensitive personal data within the meaning of Article 9(1) of the GDPR. In addition to the data covered by specific rules in Article 9 of the GDPR, IMY has however identified certain types of data that it considers to be particularly worthy of protection, so-called privacy-sensitive personal data. The fact that information that is covered by legal secrecy to protect the individual's circumstances shows that the legislator has made the assessment that the information needs to be protected from a privacy perspective. In this case, the type of information in question, that the complainant is a customer of Klarna, is such information that is covered by the obligation of professional secrecy, or, the so-called banking secrecy in the Banking and Finance Business Act. The e-mail correspondence to which the complaint relates included details of the complainant’s name and banking activities which can be linked to him. The fact that the personal data in question is typically covered by banking secrecy gives rise to an expected degree of confidentiality. IMY considers that the processing in question has included data that reveals that the complainant is a bank customer and that the processing in question therefore included so-called privacy-sensitive, that is to say, particularly worthy of protection, personal data.

The processing in question involved the transmission of data by e-mail over an open network where the sending server had the opportunistic TLS setting. An email protocol is designed to make the entire message arrive from the sender to the receiver. If the sending server is unable to establish a direct contact with the receiving server, the e-mail may pass through one or more other servers along the way but will eventually arrive in its entirety. If the receiving server, or any intermediate server, is not configured to use TLS, the transmission is unencrypted, which means that the e-mail message is transmitted in plain text over the open network.

[2] See Lycke, Banking and Financing Business Act (2004:297), Chapter 1, section 10, section 2.1 Those to whom the provision is directed to and those whom the confidentiality is intended to protect, Lexino 2018-07-26 (JUNO))

When an email message is sent over an open network, the sender or recipient generally has no control over which devices (such as network nodes or servers) the specific email message passes along the way. One consequence of this is that anyone who possesses equipment through which unprotected e-mails pass can access, disseminate or distort them.

When transmitting the complainant's data via e-mail, Klarna took measures in the form of an encryption solution with an opportunistic server setting to protect the data. IMY notes that this solution means that, when sending e-mails, Klarna's server has had the opportunity to negotiate an encrypted tunnel for the message to travel in. In such cases, Klarna's server has been able to exchange encryption keys with the e-mail server provided by the complainant's e-mail provider (the complainant's e-mail provider's server). However, Klarna was unable to verify or ensure, by means of the server used at the time of sending the email, that an encrypted transmission of the data at issue could be established to the complainant's e-mail provider's server. In the event that the servers of Klarna and the complainant's e-mail provider's server were unable to establish encryption, the email was sent unencrypted, that is to say, in plain language. Furthermore, even if encryption had taken place, it would have covered only the transmission of the message itself. Encryption has either ceased when it reached the complainant's e-mail provider's server or has not occurred at all. If Klarna's server had instead been set to the *mandatory* TLS setting and the complainant's email provider's server had not been able to establish an encrypted tunnel, there would have been no transmission.

Klarna states that once an e-mail has reached the recipient, it is subject to the security measures of the recipient's e-mail provider. Processing of data shall be carried out in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing pursuant to Article 5(1)(f) of the GDPR. The present case concerns privacy-sensitive data. An appropriate security measure would therefore have been for the controller to ensure that those data could not be read by anyone other than the intended recipient.

In the present case, Klarna has not been able to verify how the information was finally received by the complainant. Even if TLS encryption has taken place, it has ceased before the message reaches the intended recipient and is stored on a server connected to the internet in an unencrypted state. This means that Klarna was unable to ensure that the message containing the data was encrypted until the complainant was able to read it. Furthermore, e-mail messages stored unprotected on a server are accessible to anyone who has or can gain knowledge of the e-mail user account's password or has or can gain access to an administrator account on the server. IMY therefore concludes that regardless of whether Klarna's servers had a mandatory or opportunistic TLS solution for encryption, the transmission of the data would not have taken place in such a way that only the intended recipient could have accessed the data. Klarna's encryption solution has thus not provided sufficient protection for privacy-sensitive information covered by the complaint.

Klarna has thus identified risks that the processing of privacy-sensitive personal data in e-mail entails, but has not taken sufficient measures to ensure that only the intended recipient has been able to access the personal data in the transfer in question. At the end of encryption, protection against unauthorised disclosure of or access to personal data has been insufficient. Given the privacy-sensitive nature of the personal data, there has been a considerable risk of a breach of privacy vis-à-vis the complainant.

According to recital 83 of the GDPR, a controller should take certain security measures in order to ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the type of personal data to be protected. Klarna objects that, at the time of the complaint, current security measures were considered to be a secure means of transmitting personal data by e-mail. As IMY has stated above, it is not sufficient to protect only the transfer, but also the personal data as such must be protected against unauthorised disclosure and access. This means that only the intended recipient should have been able to access the personal data in question.

In conclusion, IMY finds that, at the time of the e-mail correspondence with the complainant, Klarna has not taken appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing, since Klarna has sent e-mails containing privacy-sensitive personal data without ensuring that the encryption solution chosen protected the message all the way to the intended recipient, in this case the complainant. Against this background, IMY therefore concludes that Klarna has infringed Article 32 of the GDPR.

Klarna's new solution for managing e-mail messages
Klarna has stated that SWK, in the period after the complaint, has continuously strengthened the technical security measures they use when sending e-mails by launching a new communication solution. It is noted that the processing of personal data carried out in the context of this solution is not the subject of the complaint and is therefore not part of the current supervision.

Choice of corrective measure

It follows from Articles 58(2) and 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, it is clear from Article 83(2) which factors must be considered when deciding on an administrative fine and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148 of the GDPR, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account shall be taken of aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and relevant previous infringements.

IMY has found that Klarna has processed personal data in breach of Article 32 of the GDPR. An infringement of that provision may give rise to a fine. Klarna's breach occurred by the company in 2018 transferring privacy-sensitive personal data to the complainant by e-mail without using a sufficiently secure encryption solution that protected the message all the way from the sender to the intended recipient.

IMY’s supervision concerns the fact that Klarna sent privacy-sensitive personal data by e-mail without the use of sufficient security measures – the subject matter of the complaint. IMY has previously stated that the sensitivity of the data being processed depends on several factors. Both the type and the quantity of data processed matter. The services in question are individual data sent by e-mail concerning the complainant’s name, together with a reference number to Klarna, the amount of the investment, the current interest rate and the commitment period of the investment. In a mitigating direction, also the level of sensitivity of this data as well as the nature of the

bank account from which the data in question originated from should be considered. Klarna, via SWK, has not sent information such as bank account number or social security number. Klarna has worked to improve security in the case at hand by strengthening the technical security measures SWK uses when sending e-mails by launching a new communication solution for e-mails to the company's customers.

Overall, therefore, IMY considers that it is a minor infringement within the meaning of recital 148 of the GDPR. Klarna Bank AB must therefore be given a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement found.

Annex
Complainant’s personal data