COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-8699

IMI case register:
134712

Date:
2025-10-30

Final decision 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 (556737-0431), in its handling of the complainant's request for access and erasure dated 28 February 2021, has processed personal data in violation of:

Article 12(6) of the General Data Protection Regulation[1], by requesting more information than necessary to identify the complainant,

Article 12(2) of the General Data Protection Regulation, by not having facilitated the exercise of the complainant's rights.

The Swedish Authority for Privacy Protection issues Klarna Bank AB a reprimand under Article 58(2)(b) of the General Data Protection Regulation for these infringements.

Presentation of the supervisory case

Background to the case

The Swedish Authority for Privacy Protection (IMY) initiated supervision in case IMY-2022-7128 to investigate 28 complaints against Klarna Bank AB (Klarna). IMY subsequently decided that the continued investigation of each complaint should be conducted in separate cases.

In the present case, IMY's investigation of the complaint has been limited to the questions of whether Klarna acted in accordance with Article 12(6) of the General Data Protection Regulation when requesting information to identify the complainant, and whether Klarna facilitated the complainant's exercise of the right of access and erasure in accordance with Article 12(2) of the Regulation. The examination in this case concerns Klarna's handling of the complainant's request for access and erasure made

[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 address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

on 28 February 2021. IMY will therefore not assess whether Klarna's current general procedures for handling such requests comply with the Regulation.

The complaint in this case has been referred to IMY, in its capacity as lead supervisory authority pursuant to Article 56 of the Regulation. The referral was made by the supervisory authority in the country where the complainant lodged the complaint (Austria), in accordance with the Regulation's provisions on cooperation in cases of cross-border processing.

The proceedings before IMY have been conducted in writing. IMY has made use of the cooperation and consistency mechanisms set out in Chapter VII of the Regulation. The supervisory authorities concerned have been the data protection authorities of Austria, Hungary, Denmark, Germany, Norway, Finland, Italy, the Netherlands, Poland, Ireland, France, Estonia, and Spain.

Submission by the complainant

The complainant has essentially stated the following. On 28 February 2021, the complainant requested access to his personal data and requested that the data be erased, pursuant to Articles 15 and 17 of the General Data Protection Regulation. The complaint shows that Klarna required the following information in order to process the request:

- first and last name
- date of birth
- email address used for a purchase
- Klarna's invoice number for a purchase
- name of a store where the complainant had made a purchase
- the exact invoice amount for an order.

The complainant subsequently provided Klarna with the following information:

- credit ID
- mandate reference
- name of the store where the complainant had made the purchase.

The complainant also informed Klarna that this information would give Klarna access to his name, email address, and registered residential address, and that he would not provide any further information.

Statement by Klarna

Klarna has, in summary, stated the following regarding the issues under supervision.

Klarna received a request for access and erasure from the complainant by email on 28 February 2021, and on 1 March 2021 Klarna initiated the identification process. On 31 March 2021, the complainant was informed that the case would be closed if Klarna did not receive the information required to complete the identification.

However, in response to IMY's questions, Klarna has reviewed the case, including the documents relating to this complaint attached by IMY, and found that the complainant can now be considered identified. The requests were therefore fulfilled on 28 September 2022, by initiating the erasure process and sending an extract of the register by post.

Did Klarna have grounds to doubt the complainant's identity?

Klarna has stated that the company was granted a banking license by the Swedish Financial Supervisory Authority in June 2017. This entails, inter alia, that the company is obliged to maintain banking secrecy under Chapter 1, Section 10 of the Banking and Financing Business Act (2004:297), and thus Klarna may not unlawfully disclose individuals' relationship with Klarna as a credit institution. In addition, Klarna processes data that many customers perceive as sensitive, such as credit decisions, payment history, and information required under anti-money laundering regulations. Klarna must therefore ensure that data is not disclosed to unauthorized parties and that customers' identities are not revealed.

Beyond the provisions of data protection legislation, the requirement of banking secrecy must therefore also be taken into account when identifying data subjects in connection with requests for access or erasure. It should also be noted that financial institutions, including banks, are particularly exposed to fraud attempts of various kinds. One example is attempts to obtain personal data from third parties in order to commit identity theft. Providing personal data to an unauthorized third party would not only enable fraud to the detriment of the data subject and Klarna, but potentially also of data subjects who are customers of merchants using Klarna's payment methods. Consequently, Klarna must ensure that no personal data is exposed to unauthorized parties and, if any doubt arises, request additional data points for identification.

Klarna continuously develops its processes for identity verification to ensure that unauthorized parties cannot gain access to customer personal data.

At the time of the complainant's request, Klarna had grounds to doubt the complainant's identity because the complainant had only provided his email address and name—two of the necessary data points required under Klarna's procedure at that time to be considered identified. For that reason, Klarna was unable to fulfill the request.

What information has Klarna required to process the request?

Klarna has stated that the complainant was asked to provide the following information:

- Name
- Date of birth
- Email address

- Invoice number
- Name of a store where the complainant had made a purchase
- Telephone number (to which the password for opening the register extract could be sent).

Why was this information necessary to confirm the complainant's identity?

Klarna's identification procedure has always been based partly on the possibility of verifying a customer's identity through the customer providing a number of different data points that only the customer should know, and partly on preventing unauthorized parties from being able to guess the information required for identification. To facilitate matters for customers, Klarna indicates within the identification process the data points which, in different combinations, can be used to verify a customer's identity.

Since customers may remember different information and may have used payment methods requiring different data, Klarna provided the complete list of data points. However, not all the listed data points are needed in every individual case. Instead, different combinations of these points have been sufficient to identify the customer, depending on the time and the country in which the request was made. In cases where a customer service representative requested additional data points even though a customer had already provided enough information to be identified, the cases were incorrectly handled.

An important exception is when Klarna could not locate the customer because the information provided did not match the information in Klarna's systems. In such cases, it has, for example, been considered necessary to request an alternative email address.

In the present complaint, according to the identification procedure then applicable in Germany, Austria, Belgium, and the Netherlands, Klarna was unable to securely identify the complainant and therefore required additional information in order to ensure that the complainant's personal data would not be disclosed inappropriately. Klarna therefore specified all the information that counted as possible identification points for the complainant. Since different combinations of data are possible, Klarna informed the complainant of all data points that could be used for identification, rather than indicating a specific one.

What information was collected when the customer relationship was established, and which are new?

For identification purposes, Klarna only collects information that corresponds to data already collected.

The motivation of the decision

Applicable provisions

According to Article 12(2) of the General Data Protection Regulation, the controller shall facilitate the exercise of the data subject's rights under Articles 15–22.

Article 12(6) of the General Data Protection Regulation provides that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making a request under Articles 15–21, the controller may request the provision of additional information necessary to confirm the data subject's identity.

The European Data Protection Board's (EDPB) Guidelines 01/2022 on the right of access state the following.

Where the controller requests or receives the additional information from the data subject necessary to confirm the data subject's identity, the controller shall, on a case-by-case basis, assess what information makes it possible to confirm the identity of the data subject. The controller may, where proportionate, ask supplementary questions to the requesting person or request the data subject to provide additional identification details.

If the controller has reasonable grounds to doubt the identity of the requesting person, it may, as stated above, request additional information to confirm the data subject's identity. At the same time, the controller must ensure that no more personal data than necessary for authentication of the requesting person is collected. The controller must therefore carry out a proportionality assessment, taking into account the type of personal data being processed (e.g. whether it involves special categories of data), the type of request, the context in which the request is made, and any potential harm that could result from unlawful disclosure. In assessing proportionality, it should be borne in mind to avoid disproportionate collection of information, while ensuring an adequate level of security in processing.

The controller should implement an authentication procedure to ensure the identity of individuals requesting access to their data and to maintain security in the processing throughout the handling of an access request in accordance with Article 32 of the General Data Protection Regulation, for example by providing a secure channel through which the data subject may provide additional information. The method used for authentication should be relevant, appropriate, proportionate, and consistent with the principle of data minimisation. If the controller imposes burdensome measures aimed at authenticating the data subject, it must properly justify such measures and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Article 12(2) GDPR).

IMY:s assessment

Has Klarna acted in accordance with Article 12(6) of the GDPR when requesting the relevant information from the complainant?
Did Klarna have reasonable grounds to doubt the complainant's identity?

It is only when the controller has reasonable grounds to doubt the identity of the requester that additional information to confirm identity may be requested. What constitutes "reasonable grounds" under Article 12(6) GDPR must be assessed based on the circumstances of the individual case. The assessment is normally made in light of the information provided in connection with the request, particularly where the controller does not have closer knowledge of the person. While an individual assessment is required, this does not preclude the establishment of general routines for how the controller normally verifies a data subject's identity.

The requirements that may be placed on the information will typically be higher the more sensitive the personal data processing is. In other words, a certain type of identification information may suffice for one type of processing, but raise doubts in another.

According to the complaint, the complainant provided name and email address in connection with his request. Klarna has stated that, since the complainant only provided two of several required data points that, under its procedure at the time, were necessary to be considered identified, Klarna had reasonable grounds to doubt the complainant's identity. Furthermore, Klarna has stated that the obligation of banking secrecy, which the company is required to uphold, must be considered when identifying data subjects in connection with requests for access or erasure. Klarna also processes data that many customers regard as sensitive, and the company must therefore ensure that data is not disclosed to unauthorized persons and that customer identities are not revealed. Financial institutions are particularly exposed to various types of fraud attempts, and Klarna must ensure that no personal data is exposed to unauthorized parties and, where doubts arise, request additional data points for identification.

IMY notes that the obligation to ensure the identity of the requester aims, among other things, to protect data subjects from others wrongfully making requests in their name, which could lead to negative consequences for the data subjects. In view of the nature of the personal data processed by Klarna, and in light of the information provided by the complainant in his request for access and erasure, IMY finds no reason to question that Klarna had reasonable grounds to doubt the complainant's identity.

Were the data requested by Klarna necessary to confirm the complainant's identity?

The GDPR does not explicitly regulate what information may be requested or how the additional information should be collected. However, the principle of data minimisation in Article 5(1)(c) GDPR is central in this regard. Even if the controller has reasonable grounds to doubt the data subject's identity, it must not collect more personal data than necessary to enable identification. Routinely requiring information for identification without regard to necessity, as described in Article 12(6) GDPR, is contrary to that provision.

The controller must conduct a proportionality assessment and be able to justify the verification method used. This assessment must establish what is appropriate in light of the GDPR's requirements, including on security, as well as the obligation under Article 12(2) GDPR to facilitate the exercise of data subject rights. To avoid excessive collection of information, a request for additional data must be proportionate in relation to the type of data processed and the potential harm that may result from disclosure to the wrong person.

Klarna has stated that data subjects can be identified through various combinations of a number of data points set out in its procedure. In the identification process, all these possible data points are requested, but not all are necessary in every individual case.

According to the EDPB's Guidelines on the right of access, the controller, in making the proportionality assessment, must consider the type of personal data processed (e.g. whether it concerns special categories of data), the nature of the request, the

context in which the request is made, and any potential harm that may arise from undue disclosure.

As regards the information requested by Klarna from the complainant, IMY notes the following. Since Klarna operates as a bank, disclosure of personal data to an unauthorized party could have serious consequences for the complainant. The requirements for identification must therefore be set relatively high. Klarna also requests only information corresponding to data that the company already processes about the complainant.

However, according to Klarna itself, not all of the additional data requested were necessary to identify the complainant. IMY also notes that, at Klarna's request, the complainant submitted additional data such as Credit ID, mandate reference, and the name of the store where the purchase was made—information that, according to the complainant, would also enable Klarna to retrieve his name, email address, and registered address. Klarna has not responded to this claim, but instead, according to the complainant, continued to request the same information, including email address, name, and address.

IMY therefore finds that Klarna did not make an individual assessment of what data were necessary to identify the complainant. Routinely requesting a large amount of information for identification in the manner that occurred, without regard to necessity as described in Article 12(6) GDPR, is contrary to that provision.

Since more information than necessary to identify the complainant was requested, IMY concludes that Klarna processed the complainant's personal data in violation of Article 12(6) GDPR.

Has Klarna facilitated the complainant's exercise of his right of access under Article 12(2) GDPR?

According to Article 12(2) GDPR, the controller shall facilitate the exercise of the data subject's rights under Articles 15–22.

Klarna requested that the complainant provide certain information in order to confirm his identity and subsequently handle his request for access and erasure. For this purpose, the complainant was asked to provide, inter alia, invoice number, the name of the store where a purchase was made, and order number. As noted above, IMY has assessed that not all of the data requested by Klarna were necessary to identify the complainant. This meant that the complainant had to conduct investigations to locate several items of information, even though they were not always necessary. Against this background, IMY considers that the verification method was too burdensome for the complainant in a way that hindered the exercise of his rights of access and erasure.

IMY therefore concludes that Klarna did not facilitate the complainant's exercise of his rights as required by Article 12(2) GDPR. Klarna has thus processed the complainant's personal data in violation of Article 12(2) GDPR.

Choice of corrective measure

In cases of deficiencies, IMY may take certain corrective measures. Articles 58(2) and 83(2) GDPR provide that IMY has the power to impose administrative fines in accordance with Article 83. Where a minor infringement is at issue, Recital 148 states that, instead of imposing a fine, IMY may issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances in the case shall be considered, such as the nature, gravity and duration of the infringement, as well as any previous relevant infringements.

IMY notes the following relevant circumstances. IMY has found that Klarna requested more information than was necessary to identify the complainant. However, the information requested by Klarna did not consist of sensitive data, special categories of data, or otherwise particularly privacy-sensitive data. IMY has further found that Klarna did not facilitate the exercise of the complainant's right of access. Nevertheless, Klarna responded without delay to the complainant's email in order to address his requests for access and erasure. Although the complainant's rights of access and erasure were not fulfilled at the time of the request, but only on 28 September 2022, the shortcomings were of a less serious nature than if the complainant's request had been left entirely unanswered.

Against this background, IMY considers that the infringements in question constitute minor infringements within the meaning of Recital 148, and that Klarna shall therefore be issued a reprimand pursuant to Article 58(2)(b) GDPR for the established infringements.

This decision has been taken by Department Lawyer [redacted].

Appendix
The complainant's personal data