COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-9251

German SA's ref:
521.14807 / 631.421

IMI case register:
134712

Date:
2025-11-12

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 (IMY) establishes that Klarna Bank AB (556737-0431), in its handling of the complainant's request for access and erasure made on 21 June 2021, has processed personal data in violation of

- Article 12.6 of the General Data Protection Regulation (GDPR) [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 right.

The Swedish Authority for Privacy Protection issues Klarna Bank AB a reprimand in accordance with Article 58.2(b) of the General Data Protection Regulation for the infringements of Articles 12.6 and 12.2 of the Regulation.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision in case IMY-2022-7128[2] in order to investigate 28 complaints against Klarna Bank AB (Klarna). IMY has thereafter decided that the continued investigation of each complaint shall take place in separate cases.

IMY's investigation of the complaint in the present case 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 rights in accordance with

[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).
[2] IMY initiated supervision due to 29 complaints, but on 23 September 2023 the complainant withdrew complaint 14 (DI-2021-5908).

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

Article 12.2 of the Regulation. The assessment in this case concerns Klarna's handling of the complainant's requests made on 21 June 2021. IMY will therefore not take a position on whether Klarna's current general procedures for handling requests comply with the Regulation.

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

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

Complainant's submission

The complainant has essentially stated the following. On 21 June 2021, the complainant requested access to his/her personal data and subsequently requested that the data be erased pursuant to Articles 15 and 17 of the General Data Protection Regulation.

From the documentation submitted by the complainant, it appears that Klarna required the following information in order to process the request:

- First and last name
- Date of birth
- The email address used at the time of purchase
- Klarna's invoice number
- The name of the store where the purchase was made
- Invoice amount
- Invoice address
- Mobile phone number (in order to be able to receive the extract of records in encrypted form).

Submission from the supervised entity

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

Klarna received the complainant's requests by post on 1 July 2021 and initiated the identification process on 12 July 2021. Since the complainant did not provide the requested information, the identification process could not be completed.

Did Klarna have grounds to doubt the complainant's identity?
Klarna stated that in June 2017 the company was granted a banking licence by the Swedish Financial Supervisory Authority. This entails, among other things, that the company is obliged to maintain banking secrecy in accordance with Chapter 1, Section 10 of the Banking and Financing Business Act (2004:297), and that Klarna may therefore not unlawfully disclose individuals' relationship with Klarna as a credit institution. Furthermore, Klarna processes information that many customers perceive as sensitive, such as credit decisions, payment history, and data under the anti-money laundering framework. Klarna must therefore ensure that information is not disclosed to unauthorised parties and that customers' identities are not revealed.

In addition to the requirements of data protection legislation, the obligation of banking secrecy must also be considered when identifying data subjects in connection with requests for access. It should also be noted that financial institutions, including banks, are particularly exposed to attempted fraud of various kinds. One example is attempts to obtain personal data from third parties in order to commit identity theft. Disclosing personal data to an unauthorised third party would not only enable fraud at the expense of the data subject and Klarna, but potentially also of data subjects who have used Klarna's payment methods at online merchants. Klarna must therefore ensure that no personal data is exposed to unauthorised persons and, if doubts arise, request additional data points for identification.

Klarna is continuously developing its identity verification processes to ensure that unauthorised persons cannot gain access to customers' personal data. At the time of the request, Klarna considered that it had reason to doubt the complainant's identity. For this reason, Klarna was unable to fulfil the request.

What information did Klarna require in order to process the request?
Klarna stated that the complainant was asked to provide the following information:

- First and last name
- Date of birth
- The email address used at the time of purchase
- Klarna's invoice number
- The name of the store where the purchase was made
- The invoice address

Why was this information necessary to confirm the complainant's identity?
Klarna explained that its identification procedure has always been based on two principles: first, that a customer's identity can be verified by providing a number of different data points that only the customer should know; and second, that unauthorised persons should not be able to guess the information required for identification.

In order to simplify the process for customers, Klarna provides in the identification procedure a list of data points that can, in various combinations, be used to verify a customer's identity. Since customers may remember different information and have used payment methods requiring different details, Klarna has communicated the full

list of possible data points. However, all the information on the list is not required in every single case. Instead, different combinations of these data points have been sufficient to identify the customer, depending on when and in which country the request was made.

In cases where a customer service employee requested additional data points even though the customer had already provided enough information to be identified, the cases were handled incorrectly. An important exception is where Klarna could not locate the customer because the information provided by the customer did not match the information in Klarna's systems. In such cases, it was, for example, considered necessary to request an alternative email address.

In the complaint at hand, Klarna stated that under the identification procedure then applicable in Germany, Austria, Belgium, and the Netherlands, it was not possible to securely identify the complainant, and additional information was therefore requested to ensure that the complainant's personal data would not fall into the wrong hands. Klarna stated that in this context all additional possible data points were listed, although different combinations of these data points could be sufficient for secure identification of the complainant.

What information was collected when the customer relationship was established, and what is new?
For identification purposes, Klarna only collects information corresponding to data already collected.

Motivation for the decision

Applicable provisions, etc.

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?

Additional information to verify identity may only be requested when the data controller has reasonable grounds to doubt the identity of the person making the request. What constitutes "reasonable grounds" under Article 12.6 of the General Data Protection Regulation (GDPR) should be assessed based on the circumstances of the individual case. The assessment is normally made on the basis of the information provided in connection with the request, particularly in situations where the data controller has no prior knowledge of the requester. The requirement for an individual assessment does not preclude the establishment of general procedures for how the data controller normally verifies the identity of data subjects.

The level of information required will typically be higher the more sensitive the personal data is. In other words, a certain type of identification information may suffice in one processing context but give rise to doubts in another.

In the present complaint, the complainant provided their name and email address with the request. Klarna has stated that because the complainant only provided two of several data points required under the then-applicable procedure to be considered identified, Klarna had reasonable grounds to doubt the complainant's identity. Klarna further stated that the obligation to maintain banking secrecy, which the company is required to uphold, must be taken into account when identifying data subjects in connection with access requests. In addition, Klarna processes information that many customers perceive as sensitive, and the company must ensure that information is not disclosed to unauthorised persons and that customers' identities are not revealed. Financial institutions are particularly exposed to fraud attempts of various kinds, and Klarna must ensure that no personal data is exposed to unauthorised parties and, in case of doubt, request additional data points for identification.

IMY notes that the obligation to verify the identity of the requester is intended, among other things, to protect data subjects from someone else making requests in their name, which could lead to adverse consequences for the data subjects. In light of the nature of the personal data processed by Klarna and the information provided by the

complainant, 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 which data may be requested or how additional information should be collected. However, the principle of data minimisation under Article 5(1)(c) GDPR is central in this context. Even if the data controller has reasonable grounds to doubt the identity of the data subject, it must not collect more personal data than is necessary to enable identification. Routinely requesting data without considering whether it is necessary, as described in Article 12.6 GDPR, violates this provision.

The data controller must carry out a proportionality assessment and be able to justify the verification method used. This assessment must consider what is appropriate in light of GDPR requirements, including security, and the obligation under Article 12.2 GDPR to facilitate the exercise of data subjects' rights. To avoid excessive data collection, a request for additional information must be proportionate to the type of data processed and the potential harm that could result from disclosure to the wrong person.

Klarna has stated that data subjects can verify their identity using various combinations of a set of data points established in Klarna's procedure. During the identification process, all these possible data points are requested, but not all are necessary for identification.

According to the European Data Protection Board's (EDPB) guidelines on the right of access, the proportionality assessment must take into account the type of personal data processed (e.g., whether special categories of data are involved), the nature of the request, the context in which the request is made, and potential harm from improper disclosure.

Regarding the data requested by Klarna from the complainant, IMY notes that, given Klarna's banking activities, disclosing personal data to an unauthorised person could have serious consequences for the complainant. Therefore, the identification requirements must be relatively high.

However, according to Klarna itself, not all of the additional information requested was necessary to identify the complainant. As noted above, the data controller must make an assessment in each individual case and should not request more personal data than necessary for identification. It is not evident that Klarna made such an assessment in the complainant's case. Routinely requesting a large number of data points, as occurred here, without assessing necessity, contravenes Article 12.6 GDPR.

In light of the fact that more data was requested than necessary to identify the complainant, IMY finds that Klarna processed the complainant's personal data in violation of Article 12.6 GDPR.

Did Klarna facilitate the complainant's exercise of rights under Article 12.2 GDPR?

Under Article 12.2 GDPR, the data controller must facilitate the exercise of data subjects' rights under Articles 15–22. Klarna requested that the complainant provide certain data to verify identity and then process the requests. The complainant was asked to provide their first and last name, date of birth, email address used at the time of purchase, Klarna invoice number, the name of the store where the purchase was made, and the invoice address.

As noted above, IMY has found that not all of the data requested by Klarna was necessary to identify the complainant. This meant that the complainant had to undertake efforts to locate multiple data points, even though these were not always necessary. Against this background, IMY finds that the verification method was overly burdensome for the complainant and hindered the exercise of his rights.

IMY therefore concludes that Klarna did not facilitate the exercise of the complainant's rights as required under Article 12.2 GDPR. Klarna has consequently processed the complainant's personal data in violation of Article 12.2 GDPR.

Choice of corrective measure

Where deficiencies are identified, IMY may take certain corrective actions. Articles 58.2 and 83.2 of the General Data Protection Regulation (GDPR) provide that IMY has the authority to impose administrative fines in accordance with Article 83. In the case of a minor infringement, IMY may, instead of imposing a fine, issue a reprimand under Article 58.2(b), as indicated in recital 148. Aggravating and mitigating circumstances should be taken into account, including 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. IMY has also found that Klarna did not facilitate the exercise of the complainant's rights. However, the information requested by Klarna did not consist of sensitive, specially protected, or otherwise privacy-sensitive data. Klarna did respond without delay to the complainant's email in order to accommodate the request for access and erasure. Taken together, IMY considers the deficiencies to be of a minor nature.

On this basis, IMY finds that the infringements in question constitute minor violations within the meaning of recital 148, and that Klarna should therefore be issued a reprimand under Article 58.2(b) GDPR for the identified infringements.

This decision has been made by Legal Counsel [redacted].

Appendix
The complainant's personal data

Copy to
Data Protection Officer

How to appeal

If you wish to appeal the decision, you should write to IMY. Indicate in your letter the decision you wish to appeal and the amendment you are requesting. The appeal must be received by IMY within three weeks of the date on which you received the decision. However, if you are a party representing the public, the appeal must be received within three weeks of the date of notification of the decision. If the appeal has been received in due time, IMY will forward it to the Administrative Court in Stockholm for consideration.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The contact details of the authority can be found on the first page of the decision.