COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-8257

German ref:
521.13796 /631.321

IMI case register:
134712

Date:
2025-12-02

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 (IMY) finds that Klarna Bank AB (556737-0431) in its handling of the complainant's request for erasure made on August, 10 2020 has processed personal data in breach of

- Article 12(6) General Data Protection Regulation (GDPR)[1] by requesting more data than is necessary to identify the complainant
- Article 12(2) of the GDPR by not facilitating the exercise of the complainant's right.

The Swedish Authority for Privacy Protection issues a reprimand to Klarna Bank AB pursuant to Article 58(2)(b) of the GDPR for the infringements of Articles 12(6) and 12(2) of the GDPR.

Presentation of the supervisory case

Background and demarcation

The Swedish Authority for Privacy Protection (IMY) has initiated supervision in case with Swedish reference number IMY-2022-7128 to investigate 28 complaints[2] against Klarna Bank AB (Klarna). Subsequently, IMY has decided that the further investigation of each complaint will take place in separate cases.

IMY's investigation of the complaint in the case at hand has been limited to the questions whether Klarna has acted in accordance with Article 12(6) GDPR when Klarna requested data to identify the complainant and facilitated the complainant's exercise of his right to erasure in accordance with Article 12(2) GDPR.

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 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 in response to 29 complaints but on 23 September 2023 the complainant withdrew complaint 14 (DI-2021-5908).

The investigation of this case concerns Klarna's handling of the complainant's request for erasure made on August, 10 2020. IMY will therefore not take a position on whether Klarna's current, general procedures for handling requests comply with the General Data Protection Regulation.

The complaint in the case has been submitted to IMY, as lead supervisory authority under Article 56 GDPR. The transfer has taken place from the supervisory authority of the country where the complainant has lodged his complaint (Germany) in accordance with the provisions of the Regulation on cooperation in cross-border processing.

The proceedings at IMY were conducted by exchange of letters. IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. 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.

Statement by the complainant

The complainant has primarily stated the following. On August, 10 2020, the complainant requested that Klarna should erase all data concerning him that the company processed. When Klarna acknowledged receipt of the request, Klarna asked him to provide several pieces of information by e-mail. The complainant then repeated the request for erasure by letter to Klarna dated August, 12 2020. According to the complainant, he had already submitted all the relevant information to Klarna on August, 3 2020.

The complainant provided the following information in emails sent to Klarna on August, 3 and 12 2020:

- surname and first name
- e-mail address
- the name of a shop purchased by the complainant.

Klarna has requested the following information from the complainant in order to deal with his request:

- surname and first name
- date of birth
- e-mail address used for purchases at Klarna
- invoice number
- name of a shop from which the complainant made a purchase true Klarna
- the amount of an invoice.

Statement by the controller

In summary, Klarna has stated the following about the issues covered by the supervision in this case.

Klarna received a request for erasure from the complainant on August, 10 2020. Klarna started an identification process on August, 11. The complainant has been informed that the case will be closed if the requested information is not received. Since the complainant has not returned this information, the identification process could not

be completed. In connection with IMY's supervisory case, Klarna initiated erasure on October, 6 2022 and thus complied with the request.

Has Klarna had reason to doubt the complainant's identity?
Klarna has stated that in June 2017 the company was granted a banking license by the Swedish Financial Supervisory Authority. This means, 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 must therefore not unlawfully disclose individuals' relationship with Klarna as a credit institution. In addition, Klarna processes information that many customers perceive as sensitive, such as credit decisions, payment history and information according to the anti-money laundering regulations. Klarna therefore needs to ensure that information is not disclosed to unauthorised persons and that the identity of customers is not revealed. Therefore, in addition to the provisions of data protection law, the requirement of banking secrecy must also be taken into account when identifying data subjects in the context of access or erasure requests. Furthermore, it should be noted that financial institutions, such as, inter alia, banks, are particularly vulnerable to fraud attempts of various kinds. One example is attempts to obtain personal data from third parties that enable identity theft. Providing personal data to an unauthorized third party would not only enable fraud at the expense of the data subject and Klarna, but potentially also on the data subjects of online merchants who have used one of Klarna's payment methods. Consequently, Klarna must ensure that no personal data is exposed to unauthorized persons and, in case of doubt, ask for additional data points for identification.

Klarna continuously develops its identity verification processes to ensure that unauthorized persons cannot access customers' personal data.

At the time of the request, Klarna had reason to doubt the identity of the complainant, since the complainant had only provided his name and e-mail address, i.e. two of the necessary data points to be considered identified according to the current routines. For this reason, Klarna has not been able to fulfil the request.

What information has Klarna required to handle the request?

- Klarna states that the complainant was asked to provide the following information:

- date of birth
- e-mail address
- invoice number
- name of a shop from which the complainant made a purchase true Klarna
- order number.

The complainant has also been asked to provide a telephone number in order to send password for opening the register extract.

Why was the information necessary to confirm the identity of the complainant?
Klarna's identification routine has always been based on the premise that a customer's identity can be verified by the customer providing a number of different data points that only the customer should know about, and to prevent unauthorised persons from guessing the information required for identification. In order to simplify for customers, Klarna states within the identificationprocess the points that in different combinations can be used to verify a customer's identity. Since customers can remember different

data and have used payment methods that require different data, Klarna has provided the complete list of data points. However, not all information from the list is needed in each individual case. Instead, different combinations of these points have been sufficient to identify the customer, depending on when in time and in which country the request was made. In cases where a customer service employee requested additional data points even though a customer had already submitted enough information to be identified, the cases have been handled incorrectly. An important exception is cases where Klarna has not been able to find the customer because the information entered by a customer has not matched the information in Klarna's system. In such cases, it has been considered necessary, for example, to request an alternative e-mail address.

In the present complaint, according to the identification procedure then in force for Germany, Austria, Belgium and the Netherlands, Klarna has not been able to carry out a secure identification of the complainant and has therefore requested additional information to ensure that the complainant's personal data does not fall into the wrong hands. In doing so, Klarna has indicated all the additional data points that count as possible data points, but different combinations of those data points have been possible for the secure identification of the complainant.

Motivation for the decision

Applicable provisions, etc.

Pursuant to Article 12(2) of the GDPR, the controller shall facilitate the exercise of the data subject's rights in accordance with Articles 15 to 22.

Article 12(6) of the GDPR states that, without prejudice to Article 11 of the GDPR, where the controller has reasonable doubts concerning the identity of the natural person making the request reffered to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The European Data Protection Board (EDPB) Guidelines 01/2022 on the right of access[3] state the following.

> In cases where the controller requests or is provided by the data subject with additional information necessary to confirm the identity of the data subject, the controller shall, each time, assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate.[4]
>
> As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as

[3] European Data Protection Board (EDPB) Guidelines 01/2022 on data subject rights – Right of access, version 2.0 (finally adopted on 28 March 2023) (EDPB Guidelines 01/2022).
[4] EDPB Guidelines 01/2022, paragraph 67.

well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.[5]

The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32 GDPR, including for instance a secure channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimization principle. If the controller imposes measures aimed at authentifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimization and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).[6]

Assessment

Has Klarna acted in accordance with Article 12(6) of the GDPR when Klarna requested up-to-date information from the complainant?

Has Klarna had reasonable grounds to doubt the identity of the complainant?
It is only where the controller has reasonable doubts about the identity of the person making the request that further information to confirm the identity may be requested. What constitutes 'reasonable grounds' in Article 12(6) GDPR should be assessed in the light of the circumstances of the individual case. The assessment of whether there are reasonable grounds in an individual case to doubt the identity of the person making the request is normally made in the light of the information provided in connection with the request. This is particularly true in situations where the controller has no detailed knowledge of that person. However, the fact that an individual assessment is required does not preclude the establishment of procedures for how the controller normally verifies the identity of the data subject.

The requirements that can be placed on the information should typically be higher the more sensitive the personal data processing is. In other words, a certain type of identification information may be sufficient for identification in one processing operation but may give rise to doubts in another.

The complainant considers that Klarna had sufficient information to confirm his identity. However, Klarna stated that it had reasonable grounds to doubt the applicant's identity, since the applicant had provided only two of several necessary data points in order to be considered, according to the routine at the time, to be identified. Klarna also states that the requirement of banking secrecy, which it is required to maintain, must be taken into account when identifying data subjects in connection with requests for access or erasure. In addition, Klarna processes information that many customers perceive as sensitive and the company thus needs to ensure that information is not disclosed to unauthorized persons and that customers' identity is not revealed. Financial institutions are particularly vulnerable to fraud attempts of various kinds and Klarna must ensure that no personal data is exposed to unauthorized persons and, in case of doubt, ask for additional data points for identification.

[5] EDPB Guidelines 01/2022, paragraph 70.
[6] EDPB Guidelines 01/2022, paragraph 71.

IMY notes that the purpose of the obligation to ensure the identity of the person making the request is, inter alia, to protect data subjects against the wrongful making of requests in their name by another person, which may lead to negative consequences for data subjects. In the light of Klarna's submissions, in particular as regards the nature of the personal data that Klarna processes, and having regard to the information provided by the complainant in its request for erasure, IMY considers that there is no reason to question that Klarna had reasonable grounds to doubt the complainant's identity.

Has the information requested by Klarna been necessary to confirm the identity of the complainant?
The GDPR does not explicitly regulate which data may be requested or how the additional information is to be collected. However, the principle of data minimisation laid down in Article 5(1)(c) of the GDPR is central in that regard. Although the controller has reasonable grounds to doubt the identity of the data subject, the controller shall not collect more personal data than is necessary to enable the identification of the data subject. Requiring data for identification purposes on a routine basis without regard to the necessity of the data as described in Article 12(6) GDPR is contrary to that provision. The controller must carry out a proportionality assessment and be able to justify the verification method used. The proportionality assessment must be carried out in order to determine what is appropriate in the light of the Regulation's requirements relating, inter alia, to security, but also in the light of the requirement laid down in Article 12(2) of the GDPR, according to which the controller must facilitate the exercise of the data subject's rights. In order to avoid excessive data collection, requests for additional information must be proportionate to the type of data processed and the harm that may result from the disclosure of data to the wrong person or the deletion of data relating to the wrong person.

In summary, Klarna has stated that data subjects can identify themselves through various combinations of a number of data points established in Klarna's routine. In the identification process, all of these possible data points are requested, but not all of them are necessary for the identification of the data subject. The investigation in the case shows that Klarna, in addition to the information provided by the complainant in the form of name and e-mail address, has requested four additional data points in order to be able to identify the complainant.

It follows, inter alia, from the EDPB Guidelines on the right of access that, in the proportionality assessment, the controller must take into account the type of personal data processed (e.g. special categories of data or not), the nature of the request, the context in which the request is made and any harm that may result from undue disclosure.[7]

As regards the information requested by Klarna from the complainant, IMY observes the following. Given that Klarna conducts banking activities, the fulfilment of requests made by unauthorised persons could have serious consequences for the data subjects. The requirements for identification must therefore be set relatively high. In addition, Klarna only requests information that corresponds to information that the company already processes about the complainant.

However, according to Klarna itself, not all of the additional information requested was necessary to identify the complainant. As mentioned above, the controller shall carry

[7] EDPB Guidelines 01/2022, paragraph 70.

out a case-by-case assessment and shall not request more personal data than necessary to identify the requesting data subject. It does not appear that Klarna made such an assessment in the complainant's case. To routinely require a large number of data for identification in the manner that has taken place without regard to whether the data are necessary in the manner described in Article 12(6) of the GDPR is contrary to the provision in question.

In view of the fact that more information than was necessary to identify the complainant has been requested, IMY considers that Klarna has processed the complainant's personal data in breach of Article 12(6) of the GDPR.

Has Klarna pursuant to Article 12(2) of the GDPR facilitated the exercise of the complainant's right of access?
Article 12(2) of the GDPR requires the controller to facilitate the exercise of the data subject's rights in accordance with Articles 15 to 22.

Klarna has requested the complainant to provide information on, among other things, the invoice number, the name of a shop at which the complainant had previously made a purchase and the order number. As stated above, IMY considered that not all the information requested by Klarna was necessary to identify the complainant. As a result, the complainant had to carry out research in order to find several items of information relating, inter alia, to previous purchases, even though that information was not always necessary. Against this background, IMY considers that the verification method was too burdensome for the complainant in such a way that it complicated the exercise of the right to erasure.

IMY therefore concludes that Klarna has not facilitated the exercise of the data subject's right as required by Article 12(2) of the GDPR. Klarna therefore processed the complainant's personal data in breach of Article 12(2) of the GDPR.

Choice of corrective measure

In case of deficiencies, IMY may take certain corrective actions. It follows from Article 58(2) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. In the case of a minor infringement, IMY may, as indicated in recital 148, 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 notes the following relevant facts. IMY has found that Klarna has requested more information than is necessary to identify the complainant. However, the data requested by Klarna did not consist of sensitive, particularly protective or otherwise privacy-sensitive data and only covered such data that Klarna already processes in the context of its customer relationship with the complainant. IMY also found that Klarna has not facilitated the exercise of the complainant's right to erasure. However, Klarna responded without delay to the complainant's email in order to comply with his request for erasure. Although the complainant's right to erasure was only satisfied in October 2022 when IMY initiated supervision against Klarna investigate the current complaint, the deficiencies found are to be considered as less serious than if the request had been left unanswered.

Against this background, IMY considers that these are minor infringements within the meaning of recital 148 and that Klarna is to be given a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringements found.

This draft decision has been made by Legal Advisor [redacted], after presentation by Legal Advisor [redacted].

Appendix
The complainant's personal data

Copy to
A copy of this decision will be sent to the controllers data protection officer

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

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. IMY's contact information is shown in the first page of the decision.