COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-9257

IMI case register:
134712

Date:
2025-12-29

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 dated 22 May 2020 has processed personal data in breach of:

- Article 12(6) 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 present case has been limited to the questions whether Klarna has acted in accordance with Article 12(6) of the GDPR when Klarna requested data to identify the complainant and if Klarna facilitated the complainant's exercise of its his right of erasure in accordance with Article 12(2) of the GDPR. The investigation in the case concerns Klarna's handling of the complainant's request for erasure made on 22 July 2020. IMY will therefore not take a position on

[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).

Postal address:
Box 8114
104 20 Stockholm
Sweden
Website:
www.imy.se
E-mail:
imy@imy.se
Telephone:
+46 (8) 657 61 00

whether Klarna's current, general routines for handling requests are compatible 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 the complaint (Germany) in accordance with the provisions of the Regulation on cooperation in cross-border processing.

The proceedings before 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. Relevant supervisory authorities 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 states, in essence, as follows. The complainant has no business relationship with Klarna. The complainant has therefore requested that Klarna erase his personal data. Despite this, Klarna continues to process his data and sends him spam mail.

Statement by Klarna

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

Klarna is the data controller for the processing that is the subject of the complaint. Klarna received a request for deletion from the complainant by email on 22 July 2020.

Klarna has handled the request by starting the identification process on 19 July 2020. The identification process started before the request was made because the case was first initiated due to a complaint case. In an email to Klarna on 18 July 2020, the complainant asked Klarna to close the invoice that was the subject of the case first, as the complainant reached an agreement directly with the shop. The complainant also attached annexes to that email. In connection with the complainant’s request for erasure of 22 July 2020, Klarna’s customer service staff requested identifying data points from the complaint. The complainant then stated that the information requested by Klarna is set out in the annexes to the email previously sent by the complainant to Klarna. On 23 July 2020, Klarna’s customer service staff informed the complainant that the annexes could not be opened and again asked for the identifying data points.

Has Klarna had reason to doubt the identity of the complainant?
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.

Klarna had reason to doubt the complainant's identity because it received only two of the three necessary identification points (e-mail address and name) in a format that could be accessed by Klarna. Klarna was therefore unable to identify the complainant in accordance with the procedure in force at the time. The complainant refers to an annex which he sent with his request, in which the personal data is stated to be included. Klarna's customer service representative has informed the complainant that the appendix cannot be opened and has requested the information again.

What information has Klarna required to handle the request?
Klarna states that the complainant was asked to provide the following information:

- Name
- Date of birth
- E-mail address
- Invoice number
- Name of a store they have previously purchased from
- And the date of purchase.

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.

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

When the customer relationship was established, the following personal data was collected: name, e-mail address, date of birth, telephone number and address.

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 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,

[3] European Data Protection Board (EDPB) Guidelines on the right of access – 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
[5] EDPB Guidelines 01/2022, paragraph 70.

including data minimization and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).[6]

The assessment by IMY

Has Klarna acted in accordance with Article 12(6) of the GDPR when Klarna requested additional data from the complainant?

Has Klarna had reasonable grounds to doubt the identity of the complainant?
It is only where the controller has reasonable doubts as to the identity of the requester that additional information to confirm the identity may be requested. What constitutes 'reasonable grounds' in Article 12(6) of the GDPR should be assessed in the light of the circumstances of the individual case. The assessment of whether there are reasonable grounds to doubt the identity of the requester in an individual case is normally made in the light of the information provided in the context of the request. This is particularly true in situations where the controller does not have detailed knowledge of that person. However, the need for an individual assessment does not preclude the establishment of procedures by which 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 processing of the personal data is. In other words, one type of information for identification may be sufficient for identification in the case of one processing operation but may cast doubt in the case of another.

Klarna stated that, since the complainant had provided only two of the three data points necessary to be considered identified in accordance with the procedure in force at the time, it had reasonable grounds to doubt the identity of the applicant. In addition, Klarna 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 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 the identity of customers is not disclosed. Financial institutions are particularly vulnerable to fraud attempts of various kinds and Klarna must ensure that no personal data is exposed to unauthorised persons and, if in doubt, ask for additional data points for identification.

IMY notes that the obligation to ensure the identity of the person making a request is aimed, inter alia, at protecting data subjects against the wrongful making of requests in their name by another person, which may lead to negative consequences for data subjects. IMY notes that it is clear from the investigation in the case that the complainant indeed submitted a file with identification data to Klarna in close connection with its request for deletion. However, Klarna informed the complainant that the file was not legible for the company and therefore asked him to provide further identification points. However, as far as the investigation shows, the complainant did not provide any information other than that provided in connection with his request for erasure (name and e-mail address). In view of the nature of the personal data that Klarna processes, IMY considers that there is no reason to question that Klarna had reasonable grounds to doubt the identity of the complainant.

---

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

Has the information requested by Klarna been necessary to confirm the identity of the complainant?

The General Data Protection Regulation 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 this regard. Even if the controller has reasonable doubts about 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. To routinely require data for identification without regard to whether the data are necessary in the manner described in Article 12(6) of the 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 is to facilitate the exercise of the data subject's rights. In order to avoid excessive data collection, a request for additional information must be proportionate to the type of data being processed and the harm that may result from the disclosure of data to the wrong person.

In summary, Klarna has stated that data subjects can identify themselves through different 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. Klarna states that, in the complaint at issue, in addition to her email address, Klarna asked the complainant to provide five additional data points in order to identify her.

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 damage that may result from undue disclosure.[7] Although the complaint at issue concerns the right to erasure, IMY nevertheless considers that those guidelines provide guidance for the interpretation of Article 12(6) of the GDPR in the present case.

Klarna, among other things, stated the following. Data subjects can identify themselves through various combinations of a number of data points defined in Klarna's routine. In the identification process, all these possible data points are requested but not all are necessary for the identification of the data subject. Klarna has requested additional personal data from the complainant to ensure secure identification. Klarna has in its request requested all additional data points that are counted as possible data points.

IMY initially considers that the requirements for identification, in terms of the nature of the personal data that Klarna processes and the negative consequences that may arise if a handling of a request from an unauthorized person may have, must be set relatively high. IMY therefore does not dispute that Klarna may have needed more information to identify the complainant. However, Klarna states that not all the information it requested from the appellant was necessary to identify the complainant. As mentioned above, the controller shall make an assessment on a case-by-case basis and shall not request more personal data than is 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

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

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 data 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 erasure?

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.

Klarna has requested the complainant to provide information on, inter alia, the invoice number, the name of a shop at which the complainant had previously made a purchase and several other information. As stated above, IMY considered that not all the information requested by Klarna was necessary to identify the complainant. This has meant that Klarna has required the complainant to carry out research to find more information on, inter alia, previous purchases, even though this information was not always necessary, in order to have its request satisfied. Against that background, IMY considers that the verification method was too burdensome for the complainant in such a way as to make it more difficult to exercise the right to erasure.

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

Choice of corrective measure

It follows from Article 58(2) and Article 83(2) of the GDPR that the 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 taken into account when deciding on an administrative fine and when determining the amount of the fine. In the case of a minor infringement, as set out in recital 148, instead of imposing a fine, IMY may 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 had not facilitated the exercise of the complainant's right to erasure. However, Klarna responded without delay to the complainant's request in order to comply with his request for erasure, which means that the deficiencies found may be considered less serious than if the request were left unanswered.

In an overall assessment of the circumstances of the present case, IMY considers that Klarna should be given a reprimand for the infringements found.

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

Appendix
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.