COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-8259

IMI case register:
134712

Date:
2025-12-02

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 handling of the case

IMY has initiated supervision against Klarna Bank AB (Klarna or the company) in case IMY-2022-7128 due to several complaints against the company, including the complaint in the present case. IMY has subsequently decided to continue processing the present complaint in a separate case with a new case number, IMY-2025-8259. As a consequence, previous communication in the current case has been conducted through letters with case number IMY-2022-7128.

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.

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).

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. On 22 May 2020 the complainant sent a letter to request access to his personal from Klarna. In the context of its request, the complainant provided the following information:

- First and last name
- E-mail address
- Postal address
- Phone number.

The complainant also attached a copy of his identity card to his application. On 12 June 2020, Klarna contacted him by email and asked for more information, even though that information should have been available to Klarna. Klarna requested, inter alia, the complainant's name, telephone number, email address, date of birth as well as information about Klarna's customer (IKEA). The Complainant replied to the questions on the same day to the extent possible, stressing that he expected a response to the request by 22 June 2020. Nevertheless, Klarna did not comply with the 's request for access.

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 access from the complainant on 29 May 2020 (dated 22 May 2020). The request started to be processed on 12 June 2020. On 7 August 2020, after questions were answered regarding the credit reports allegedly initiated by Klarna and a discussion about the identification process continued, Klarna informed that the information provided by the applicant was not sufficient to identify the applicant. As a result, the request could not be fulfilled.

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. 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 had reason to doubt the identity of the complainant as it was unable to verify the data points (e-mail address, name, date of birth, telephone number and name of shop) provided by the complainant. As a result, Klarna is unable to identify the complainant in accordance with the company’s procedures. For this reason, Klarna has not been able to comply with the request.

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

- Name
- E-mail address that was used for the purchase
- Date of birth
- Invoice number
- Order number
- Name of shop.

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.

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.

Date of birth has been a mandatory data point for identifying customers at the time of the case. Klarna's procedures are constantly evaluated and developed, and for data protection cases, the date of birth is no longer a mandatory data point for identification in Germany. Klarna therefore currently has enough information to identify the complainant in accordance with our procedures. Klarna therefore intends to contact the complainant to see if the request is still up-to-date and, if so, provide the complainant access.

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[2] 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.[3]
>
> 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.[4]

---

[2] 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).
[3] EDPB Guidelines 01/2022, paragraph 67
[4] EDPB Guidelines 01/2022, paragraph 70.

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 states that the company was not able to verify the data points provided by the complainant in connection with the request and that, as a result, it did not have the information necessary to identify the applicant in accordance with the procedure in force at the time. 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 access or deletion. 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.

Klarna also stated that it did not have the complainant's date of birth and that this was mandatory under the identification procedure in force at the time. On the other hand, the complainant claims that the date of birth is apparent from his initial request. It is apparent from the file that the applicant stated in his request dated 22 May 2020 that complainant attached a copy of his identity card. It is also apparent from the file that, in the email sent to Klarna on 12 June 2020, the complainant stated that the date of birth appeared in the request. However, Klarna maintains that it does not have the date of birth of the complainant.

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 erroneous making of requests in their name by someone else, 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 processed by Klarna, and in the light of the information provided by the complainant in its request for access, IMY considers that there is no reason to doubt that Klarna had reasonable grounds to doubt the complainant's identity. Furthermore, IMY notes that there is no evidence that the complainant has submitted a copy of his identity card in connection with the request. In the light of the foregoing, IMY considers that there is no reason to question that Klarna had reasonable grounds to doubt the identity of the complainant.

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.[5]

As regards the information requested by Klarna from the complainant, IMY notes the following. In view of the fact that Klarna carries out banking activities, the disclosure of personal data to an unauthorised person could have serious consequences for the complainant. The identification requirements must therefore be set relatively high. Klarna also 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 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.

---

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

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 access?
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.

IMY considers that the verification method was burdensome for the complainant in such a way as to make it more difficult to exercise the right of access. In making that assessment, IMY took into account, in particular, the fact that Klarna had requested information which was already apparent from the complainant's initial request and that not all the information requested by Klarna had been necessary to identify the appellant in the individual case.

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 of access. However, Klarna responded without delay to the complainant's letter in order to comply with her request for access. Klarna has also stated that it now intends to contact the complainant to see whether the request is still valid and, if so, to send an extract from the register to the complainant.

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 Legal Counsel [redacted] after presentation by legal advisor [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.