COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-8258

Case number DE SA:
521.13815/631.318

IMI case register:
CR134712

Date:
2025-10-17

Final 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 requests to exercise rights under the GDPR[1] has processed the complainant's personal data in breach of

- Article 12(6) GDPR 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.

IMY issues a reprimand to Klarna Bank AB pursuant to Article 58(2)(b) of the GDPR for the infringements.

Presentation of the supervisory case

Background and demarcation

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) GDPR when Klarna has requested information to identify the complainant and whether Klarna has facilitated the complainant's exercise of its rights under the GDPR in accordance with

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).

Article 12(2) GDPR. IMY will therefore not take a position on whether Klarna's current, general procedures for handling requests are compliant with the GDPR.

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 main points of the complaint are as follows. On 10 July 2020, the complainant contacted Klarna because someone had hacked the complainant’s account with a cinema chain and ordered tickets on invoice in the complainant’s name. The complainant informed Klarna that the complainant had not ordered the tickets in question and that he therefore objected to the claim sent to him by Klarna. The complainant’s e-mail to Klarna shows the complainant’s e-mail address and first and last name.

It is apparent from the documents in the complaint that Klarna requested the following information in order to further assist the complainant:

- Surname(s) and first name(s)
- Date of birth
- E-mail address
- Invoice number
- Address
- Name of the shop purchased by the complainant
- Date of order.

Klarna has also stated that it only provides information on the invoice to which it is addressed.

The complaint shows that the complainant questions the provision of such personal and sensitive information by unencrypted email and why it would be necessary to assist him further.

Statement by Klarna

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

By letter of 27 October 2020, Klarna received a request for access from the complainant. The letter was dated 21 October 2020. Klarna has started the identification process on 27 October 2020. Klarna has asked the complainant to provide additional data points, which the complainant has done. The identification process was completed on 4 November 2020 and Klarna sent a copy of the complainant’s personal data to the complainant by post on 23 November 2020.

Has Klarna had reason to doubt the identity of the complainant?
Klarna has stated that the company was granted a banking licence by the Swedish Financial Supervisory Authority in June 2017. 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 deletion requests. Furthermore, it should be noted the fact 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 data subjects of online merchants who have used one of Klarna's payment methods. Consequently, Klarna must ensure that no personal data is disclosed to unauthorised 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 enquiry, Klarna had reason to doubt the complainant's identity, since the complainant had provided only his name and e-mail address, i.e. two of the data points necessary to be regarded as identified in accordance with the procedure in force at the time. Since the complainant has provided additional data points, he has been identified and Klarna has sent him a copy of his personal data.

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 has made a purchase
- Exact invoice amount
- Phone number.

Why was the information necessary to confirm the identity of the complainant?
Klarna's identification routine has always been based on the assumption that a customer's identity can be verified by the customer providing a number of different data points that only the customer should be aware of, and to prevent unauthorized persons from guessing the data required for identification. In order to simplify for customers, Klarna states in the identification process the points that in different combinations can be used to verify a customer's identity. Since customers can remember different information and have used payment methods that require different information, Klarna has provided the complete list of data points. However, not all information from the list is required in each 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 the present complaint, according to the then applicable identification procedure 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 to the complainant all the additional data points that are counted as possible data points, but different combinations of those data points have been possible for the purposes of secure identification.

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

Motivation of 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 provides that, without prejudice to Article 11 of the GDPR, where the controller has reasonable doubts as to the identity of the natural person making a request referred 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]
>
> Where the controller has reasonable grounds to doubt the identity of the requesting person, it may, as indicated above, request additional information to confirm the identity of the data subject. Nevertheless, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable the authentication of the requesting person. To that end, the controller shall carry out a proportionality assessment that takes into account the type of personal data processed (e.g. special categories of data or not), the type of request, the context in which the request is made, and any harm that could result from undue disclosure. When assessing proportionality, it should be remembered to avoid unreasonable data collection while ensuring an adequate level of security of processing.[5]
>
> The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data34, and

[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.

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

The assessment by IMY

It is apparent from the e-mail conversation attached to the complaint that the complainant contacted Klarna on 10 July 2020 to inform Klarna that he had been the victim of fraud and therefore opposes the claim in an invoice sent to him by Klarna. It can be inferred from Klarna's reply that Klarna perceived the complainant's message as a request for access to information on the data in the relevant invoice and therefore requests additional information in order to be able to help him further.

In connection with IMY's investigation of the complaint, Klarna did not adress the email correspondence Klarna had with the complainant in July 2020. However, Klarna states that, on 27 October 2020, it received a request for access and deletion from the complainant and that, in that context, Klarna requested additional information from the complainant in order to identify him. On 23 November 2020, when the complainant had submitted the necessary data for identification, Klarna sent the complainant a copy of his personal data by post and informed him that the deletion process had started.

IMY intends to examine whether Klarna, when handling the complainant's requests, had support for requesting additional information to confirm the complainant's identity and whether Klarna facilitated the exercise of the complainant's rights.

Has Klarna acted in accordance with Article 12(6) of the GDPR when Klarna requested additional 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 as to the identity of the person making the request that additional 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 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, a certain type of information for identification may be sufficient for identification in one case of processing but may cast doubts in the case of another.

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

The investigation in the case shows that the complainant, in its initial contacts with Klarna in connection with its requests, provided its first and last name and e-mail address. Klarna states that Klarna had reasonable doubts as to the complainant's identity, since the complainant had provided only two of several necessary data points which, according to the current routine, were required for him to be considered identified. 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 therefore 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 disclosed to unauthorised persons and, if in doubt, ask for additional data points for identification.

IMY assesses 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 someone else, which may lead to negative consequences for data subjects. In the light of Klarna's submissions, including as regards the nature of the personal data that Klarna processes, and having regard to the information provided by the complainant in its requests, IMY considers that there is no reason to question Klarna's statement that Klarna initially 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 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 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. 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 requirements of the Regulation, including those relating to security, but also in the light of the requirement in Article 12(2) of the GDPR, according to which the controller shall facilitate the exercise of the rights of the data subject. In order to avoid excessive data collection, a request for additional information must be proportionate to the type of data processed and the harm that may occur when disclosing data 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 these possible data points are requested but not all are necessary for the identification of the data subject. The investigation in the case shows that Klarna, in the complaint at issue, in connection with the complainant's requests, asked the complainant, in addition to his name and e-mail address, to provide five additional data points in order to identify him.

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 notes the following. Given that Klarna carries out banking activities, the disclosure of personal data to an unauthorised person could have serious consequences for the complainant. The requirements for identification must therefore be set relatively high. In addition, Klarna only requests information that corresponds to information that it already processes about the complainant.

However, according to Klarna itself, not all of the additional information requested was necessary to identify the appellant. 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 appellant's case. Requiring, as a matter of routine, a large number of data for identification purposes in the manner that has taken place without regard to the necessity of the data as described in Article 12(6) of the GDPR is contrary to the provision in question.

In view of the fact that more information than is 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 rights?
According 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 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 to find more information on, inter alia, previous purchases, even though this 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 complainant's rights.

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 infringements, IMY may take certain corrective measures. 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

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

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 found that Klarna had requested more information than was necessary to identify the complainant. However, the data requested by Klarna did not consist of sensitive, particularly protective or otherwise privacy-sensitive data and covered only such data that Klarna is already processing about the complainant. IMY further notes that Klarna has not facilitated the exercise of the complainant's rights. However, Klarna responded without delay to the complainant's emails in order to comply with his requests. In addition, it should be noted that the complainant's request made in October 2020 was complied with within the time limit laid down in Article 12(3) of the GDPR. The breaches found are therefore less serious than if the complainant's requests had been left unanswered.

In the light of the foregoing, IMY considers that these are minor infringements within the meaning of recital 148 and 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 taken by the departmental lawyer [redacted] after a presentation by the departmental lawyer [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.