COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-8244

German ref.:
521.13793/631.332

IMI case register:
CR134712

Date:
2025-10-29

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 requests for access made on 10 December 2018 and 9 July 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 rights.

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.

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).

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 been able to identify data referring to the complainant, if the company has acted in accordance with Article 12(6) of the GDPR when Klarna requested data to identify the complainant and facilitated the complainant's exercise of its right of access in accordance with Article 12(2) of the GDPR. The investigation in the case concerns Klarna's handling of the complainant's requests for access made on 10 December 2018 and 9 July 2020. IMY will therefore not take a position on 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 requested access to her personal data under Article 15 of the GDPR but Klarna has requested additional and more personal data than necessary to meet her requests. The complainant has provided the information she has had access to and has been in their systems for at least one purchase that she has made.

Request on 10 December 2018
On 10 December 2018, the complainant requested access to her personal data by e-mail and provided the following information:

- First and last name
- E-mail address.

Correspondence between the complainant and Klarna shows that Klarna has requested the following information in order to handle her request:

- First and last name

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

- Date of birth
- E-mail address used for a purchase with Klarna
- Klarna invoice number for one of the orders
- Name of a trader the complainant placed an order with
- Exact invoice amount for one of the orders.

Klarna has also required the complainant's telephone number to send a password to the complainant in order to open a copy of the personal data.

In her reply to Klarna, the complainant reiterated her first name and last name, stated her date of birth and that she did not have any more of the information requested. Klarna then replied that the company could not find her in their systems and that she will need return with details of another e-mail address she used for purchases or other personal data provided by her. The complainant informed Klarna that she is unable and unwilling to list all the e-mail addresses she uses.

Following further correspondence between the complainant and Klarna, it is shown that Klarna requested the following information from the complainant:

- E-mail address used for a purchase with Klarna
- Klarna invoice number for one of the orders
- Name of a trader the complainant placed an order with
- Exact invoice amount for one of the orders.

Request on 9 July 2020
On 9 July 2020, the complainant again requested access to her personal data. In her request, which was made via an e-mail address other than the first request, the complainant provided the following information:

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

From correspondence between the complainant and Klarna following the request shows that Klarna requested the following information to handle the request:

- First and last name
- Date of birth
- E-mail address used for a purchase with Klarna
- Klarna invoice number for one of the orders
- Name of a trader the complainant placed an order with
- Exact invoice amount for one of the orders.

Klarna has also required a telephone number to send a password to the complainant in order for her to be able to open a copy of the personal data. Klarna also requested the transaction ID and the IBAN number in the event that the complainant made use of Klarna Open Banking via a third-party provider and access to the personal data stored with it.

In her reply to Klarna, the complainant again provided her first and last name together with date of birth, an invoice number, the name of a trader she placed an order with and the exact amount of the invoice. The complainant also stated that, as far as she could see, did not use e-mail for the purchase in question. Klarna then replied that the complainant had to provide a telephone number to be able to send her a password and her to open the copy of the personal data.

After the complainant provided her telephone number, Klarna informed her that they were unable to identify her in their system and asked her to provide another e-mail address and other personal data that she had used.

Klarna then sent another e-mail to the complainant, stating that they were unable to identify her in their systems and that the company therefore could not act on her request until she had been identified and that they would stop communicating with her if she did not provide the information requested.

Statement by Klarna

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

Request on 10 December 2018
Klarna received the complainant's request for access by e-mail on 10 December 2018 and started the identification process on 12 December 2018. The complainant had provided the date of birth and name, in addition to the e-mail address from which the complainant sent the request. Klarna was unable to verify the provided e-mail address in its systems, of which the complainant was informed. Klarna asked the complainant if she had used a different e-mail address in connection with a purchase, but the complainant did not wish to share more of her e-mail addresses. Klarna has informed the complainant that more data points were required to identify the complainant, which she objected to.

Request on 9 July 2020
Klarna received the complainant's request for access by e-mail on 9 July 2020 and started the identification process on the same day. Klarna and the complainant have corresponded several times. The complainant has provided some information, but since the customer service agent did not find the complainant in the Klarna systems, the person has asked for another e-mail address through which the complainant may have made the purchases. The complainant disputed this request. Klarna has again informed the complainant that the request cannot handled until the complainant provides the information. The complainant has not provided any further information and the request could not therefore not be met. Following IMY's supervisory letter, Klarna has examined the case and found that the complainant can now be considered to be identified.

In the context of meetings between Klarna and the supervisory authority in Berlin from June to August 2021, a copy of the complainant's personal data was sent to the complainant by post on 26 August 2021.

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 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 only provided her name and date of birth, i.e. two of the necessary data points to be considered identified according to the current routine. Klarna has not been able to verify the e-mail address provided by the complainant. 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 trader the complainant placed an order with
- Order number.

The complainant has also been asked to provide the telephone number so that Klarna could send the complainant a password to open a copy of the personal data.

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?
Klarna has no customer relationship with the complainant and has not found any information on previous customer relationships. For identification purposes, Klarna does however only collect data corresponding to the data already collected.

Motivation for the decision

Applicable provisions, etc.

According to Article 11(2) of the GDPR, where, in the cases referred to in paragraph 1 of the article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall, if possible, inform the data subject accordingly. In such cases, Articles 15 to 20 shall not apply except where the data subject for the purpose of exercising its rights under those articles provides additional information enabling the identification.

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 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.

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. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify 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

[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

> 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 assessment by IMY

In order to ensure the security of processing and minimise the risk of unauthorised disclosure of personal data, the controller must be able to both find out which data refer to the data subject (identification) and also confirm the identity of that person (authentication).[6]

In the present case, Klarna has stated that it was neither able to identify data referring to the complainant nor to verify the complainant's identity.

Has Klarna been able to identify data referring to the complainant?
Klarna states that, on the basis of the information provided in the complainant's requests for access to personal data, it was not able to identify data referring to the complainant because the e-mail addresses provided could not be verified. IMY finds no reason to question Klarnas statement in this part. Furthermore, it is apparent from supporting documents that Klarna informed the complainant that they had not been able to find her in their systems and that the complainant had not provided additional information enabling an identification.

Klarna has thus shown that it was not in a position to identify data referring to the complainant and, therefore, to act on the complainant's requests for access to her personal data on the basis of Article 11(2) of the GDPR.

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?
Controllers have in the context of Article 12(6) GDPR, and without prejudice to Article 11 under the previous section, the possibility to request additional information in order to confirm the identity of the data subject's and be able to fulfil requests of rights.

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

[5] EDPB Guidelines 01/2022, paragraph 70.
[6] EDPB Guidelines 01/2022, paragraph 58.

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.

The complainant states that she, regarding the first request, provided her e-mail, first and last name and date of birth, and that she, regarding the second request, made from another e-mail address, provided her first and last name, e-mail address and postal address. She has further, with regards to the second request, provided additional information about one of the made purchases. Klarna states, as may be understood, that the complainant at the time of the first request, only provided her name and date of birth and that the complainant, regarding the second request, also provided certain other requested information. Klarna has however had reasonable doubts as to the identity of the complainant as the complainant only provided only some of the data points necessary for the identification in accordance with the procedure in force at the time.

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.

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 also 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 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 e-mail 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]

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. Supporting documents submitted by the complainant shows that Klarna repeatedly requested additional information (including at least six data points) in order to handle the request for access and that, in doing so, it also requested information which the complainant had already provided in connection with her requests. 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.

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.

Klarna has requested the complainant to provide information on, inter alia, the invoice number, the name of a trader the complainant placed an order with and the exact invoice amount. As can be seen 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

---

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

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 of access.

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. 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 e-mails in order to comply with her requests for access. Although the complainant's right of access was only granted in August 2021 in the context of meetings between Klarna and the Berlin supervisory authority, the deficiencies found are of a less serious nature than if the request had been left unanswered.

In the light of the foregoing, IMY takes the view that these are minor infringements within the meaning of recital 148 that require Klarna to be given a reprimand under Article 58(2)(b) of the GDPR for the infringements found.

This decision has been approved by [redacted], Department Lawyer, following a presentation by [redacted], Legal Advisor.

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.