COMPLAINANT
See Appendix

CONTROLLER
Klarna Bank AB

Ref number:
IMY-2025-8702

German SA case number
521.14587/631.391

Case register in IMI:
134712

Date:
2025-11-28

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 (IMY) notes that Klarna Bank AB (556737-0431) in its handling of the complainant's request for access made on 28 May 2021 has processed personal data in breach of the following articles in the General Data Protection Regulation[1] (GDPR):

- Article 12(6) GDPR by requesting more information than is necessary to identify the complainant
- Article 12(2) of the GDPR by failing to facilitate the exercise of the complainant's right.

IMY issues Klarna Bank AB a reprimand 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 delimitation

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

IMY's investigation of the complaint in the case at hand (IMY-2025-8702) has been limited to the questions whether Klarna has acted in accordance with Article 12(6) GDPR when Klarna requested information to identify the complainant, facilitating the complainant's exercise of its right of access in accordance with Article 12(2) GDPR.

The examination of the case concerns Klarna's handling of the complainant's request for access made on 28 May 2021. IMY will therefore not take a position on whether

[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 oversight following 29 complaints, but on 23 September 2023, the complainant withdrew complaint 14 (DI-2021-5908).

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

Klarna's current, general procedures for handling requests comply with the General Data Protection Regulation.

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

The proceedings at IMY were conducted by exchange of letters. IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities of Austria, Hungary, Denmark, Germany, Norway, Finland, Italy, the Netherlands, Poland, Ireland, France, Estonia and Spain.

Statement by the complainant

The complainant states, in essence, the following. On 28 May 2021, the complainant requested access to his personal data pursuant to Article 15 of the GDPR. According to the complainant, it did not comply with that request.

The documents submitted by the complainant show the following. In its request, the complainant provided the following information:

- Surname(s) and first name(s)
- Date of birth
- E-mail address
- Address.

On 29 May 2021, Klarna requested the complainant to provide the following information in order to handle the request:

- Date of birth
- E-mail address
- Invoice number
- Name of a shop purchased by the complainant
- Phone number
- Transaction ID and IBAN number in the event that the complainant has used Klarna Open Banking via a third-party provider and wishes to have access to the personal data stored with it.

The complainant has objected to the submission of further personal data and requested an explanation as to why Klarna needs information on, for example, invoice numbers in the event of a request for access. On 4 June 2021, Klarna stated that it had an obligation to identify its customers under Article 11(2) of the GDPR before complying with a right request under Articles 15 to 20 of the GDPR. In its reply, Klarna also asked the complainant for the following information:

- Invoice number
- Name of a shop where the complainant made a purchase
- Invoice amount
- Phone number to be able to send the data via a secure contact route.

Statement by Klarna Bank AB

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

Klarna received the complainant's request for access by email on 28 May 2021 and started the identification process on 29 May 2021. The process could not be completed due to the lack of additional information provided by the complainant. According to Klarna, the email address provided did not exist in Klarna's system, which is why they requested additional information. The complainant must also be informed of this in connection with a purchase on 10 June 2021.

Klarna also states that the complainant sent them an email dated 14 November 2021, referring to a letter he received from Klarna on 12 November 2021. The letter states that Klarna requested additional identification points. In the email, the complainant states that he has already provided the data in question, to which Klarna replied that no data relating to the email address provided by the complainant could be found. Klarna asked the complainant whether he had used a different e-mail address to make purchases through their service, but the complainant did not reply. Therefore, Klarna considers that the request could not be met.

Has Klarna had reason to doubt the identity of the complainant?
Klarna has stated that the company was granted a banking licence by Finansinspektionen 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 may thus 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 money laundering regulations. Klarna thus needs to ensure that information is not disclosed to unauthorised persons and that the identity of customers is not disclosed. 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 requests for access or deletion. Furthermore, attention should be drawn to 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 exposed to unauthorised persons and, if in 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 as they were unable to verify the complainant's e-mail address, name, address or date of birth, i.e. the necessary data points in order to be considered identified according to the current routine. 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:

- Date of birth
- E-mail address
- Invoice number
- Name of a store they previously made a purchase from
- Purchase price for the invoice
- 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 entering 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 cases where a customer service employee requested additional data points even though a customer had already provided enough information to be identified, the cases have been incorrectly handled. An important exception is cases where Klarna has not been able to find the customer because the information entered by a customer has not been consistent with the information in Klarna's system. In such cases, for example, it has been considered necessary to request an alternative e-mail address.

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 all the additional data points that count as possible data points, but different combinations of those data points have been possible for the purposes of the secure identification of the complainant.

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.

Grounds for the decision

Article 12(2) of the GDPR requires the controller to facilitate the exercise of the data subject’s rights in accordance with Articles 15 to 22.

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 pursuant to Articles 15 to 21, it 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.

> Where the controller requests or receives from the data subject the additional information necessary to confirm the identity of the data subject, the controller shall, on a case-by-case basis, assess what information makes it possible to confirm the identity of the data subject and, where appropriate, ask the requesting person additional questions or request the data subject to provide additional identification data, where this 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 put in place an authentication procedure to be sure of the identity of the persons requesting access to their data and to ensure the security of processing throughout the processing of an access request in accordance with Article 32 GDPR, such as a secure channel where data subjects can provide additional information. The method used for authentication should be relevant, appropriate, proportionate and consistent with the principle of data minimisation. If the controller imposes burdensome measures aimed at authenticating the data subject, it must provide appropriate justification and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Article 12(2) GDPR).[6]

Assessment by the Swedish Authority for Privacy Protection

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

Has Klarna had reasonable grounds to doubt the identity of the complainant?
It is only where the controller has reasonable doubts about the identity of the person making the request that further information to confirm the identity may be requested. What constitutes 'reasonable grounds' in Article 12(6) GDPR should be assessed in the light of the circumstances of the individual case. The assessment of whether there are reasonable grounds in an individual case to doubt the identity of the person making the request is normally made in the light of the information provided in connection with the request. This is particularly true in situations where the controller has no detailed knowledge of that person. However, the fact that an individual

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

assessment is required does not preclude the establishment of procedures for how the controller normally verifies the identity of the data subject.

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

The complainant states that he submitted his first name, surname, date of birth, address and e-mail address when he sent his request for access to Klarna. According to the complainant, Klarna failed to comply with his request for access.

Klarna states that the complainant has provided an email address that does not appear in their system. It also stated that it was unable to verify the complainant's email, name, address and date of birth, which gave the company reason to doubt the complainant's identity. 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.

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. In the light of Klarna's submissions, in particular as regards the nature of the personal data that Klarna processes, and having regard to the information provided by the complainant in its request for access, IMY considers that there is no reason to question that Klarna had reasonable grounds to doubt the complainant's identity.

Has the information requested by Klarna been necessary to confirm the identity of the complainant?
The 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 that regard. Although the controller has reasonable grounds to doubt the identity of the data subject, the controller shall not collect more personal data than is necessary to enable the identification of the data subject. Requiring data for identification purposes on a routine basis without regard to the necessity of the data as described in Article 12(6) GDPR is contrary to that provision. The controller must carry out a proportionality assessment and be able to justify the verification method used. The proportionality assessment must be carried out in order to determine what is appropriate in the light of the requirements of the Regulation, including in relation 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. Klarna states that, in the complaint at issue, it asked the complainant, in addition to his email 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 observes 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 complainant. As mentioned above, the controller must make an assessment on a case-by-case basis and not request more personal data than is necessary to identify the requesting controller. It does not appear that Klarna made such an assessment in the complaint'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 was necessary to identify the complaints 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 facilitated the exercise of the complainant's right of access under Article 12(2) of the GDPR?
Article 12(2) of the GDPR requires the controller to facilitate the exercise of the data subject's rights in accordance with Articles 15 to 22.

Klarna has requested the complainant to provide certain information by e-mail in order to be able to confirm the complainant's identity and subsequently handle the complainant's request for access further. Furthermore, the complainant has been asked to provide information on, among other things, the invoice number, the name of a shop at which the complainant had previously made a purchase and the order number. As stated above, IMY considered that not all the information requested by Klarna was necessary to identify the complainant. 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. 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 of access.

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

IMY thus 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 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. 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, Article 83(2) sets out the factors to be taken into account in deciding whether to impose an administrative fine and in determining the amount of that fine. In the case of a minor infringement, IMY may, as indicated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account shall be taken of aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and relevant previous infringements.

IMY notes the following relevant facts. IMY has found that Klarna has requested more information than was necessary to identify the complainant. However, the information requested by Klarna did not consist of sensitive, particularly worthy of protection or otherwise privacy-sensitive data and only included data that Klarna is already processing in the context of its customer relationship with the complainant. IMY further notes that Klarna has not facilitated the exercise of the complainant's right of access. However, Klarna responded without delay to the complainant's email in order to comply with his request for access.

In the light of the foregoing, IMY considers that there are minor infringements within the meaning of recital 148 that require a reprimand under Article 58(2)(b) of the GDPR for the infringements found.

This final decision has been made by the Department Lawyer [redacted] following a presentation by the 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.