

COMPLAINANT

See Annex

CONTROLLER

Klarna Bank AB

Act number:
IMY-2025-9239

**Case number of the German
Data Protection Authority**
521.14712 / 631.409

Case register in IMI:
134712

Date:
2025-11-12

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 notes that Klarna Bank AB (556737-0431) in its handling of the complainant's request for deletion and access from 11 and 18 January 2021 respectively, has processed the complainant's personal data in violation of

- Article 12(2) of the GDPR¹ by failing to facilitate the exercise of the applicant's rights.

the Swedish Authority for Privacy Protection grants Klarna Bank AB a reprimand under Article 58(2)(b) of the GDPR for the infringement.

Presentation of the supervisory case

Background and presentation

the Swedish Authority for Privacy Protection (IMY) has initiated supervision in case IMY-2022-7128 to investigate 28 complaints² 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 has been limited to the questions whether Klarna has acted in accordance with Article 12(6) GDPR when Klarna requested data to identify the complainant and whether Klarna has facilitated the complainant's exercise of its rights of access and deletion in accordance with Article 12(2) GDPR. The examination of the case concerns Klarna's handling of the complainant's request for access and deletion made on 11 and 18 January 2021. IMY

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 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 oversight following 29 complaints, but on 23 September 2023, the complainant withdrew complaint 14 (DI-2021-5908).

will therefore not take a position on whether 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 the 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 appellant submits, in essence, the following.

On 11 January 2021, the applicant requested the erasure of his personal data pursuant to Article 17 of the GDPR. In connection with the request, the appellant provided his name. The complaint shows that Klarna subsequently required the following information in order to satisfy the complainant's request:

- Surname(s) and first name(s)
- Date of birth
- E-mail address used for purchases through Klarna.

On 18 January 2021, the applicant submitted her date of birth to Klarna and, in that context, also requested access to her personal data pursuant to Article 15 of the GDPR. At the same time, the appellant states that it does not know what email address Klarna has on him and considers it irrelevant. In response to that request, Klarna sent the same reply as the complainant's first request.

Statement by the supervised entity

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

Klarna received a request for deletion from the complainant on 13 January 2021 and started the identification process on the same day. Klarna has also received a request for access by email on 22 February 2021 and started the identification process on 29 February. The applicant did not provide the information requested.

In connection with the contact between Klarna and the data protection authority in Berlin in June to August 2021, a register extract was sent to the complainant by post on 13 August 2021.

Has Klarna had reason to doubt the applicant's identity?

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 Operations 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 complainant's requests, Klarna had reason to doubt the complainant's identity, as the complainant only provided his e-mail address and his name, i.e. two of the three 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 complainant's requests.

What information has Klarna required to handle the complainant's requests?

Klarna states that the complainant was asked to provide the following information:

- Name
- Date of birth
- E-mail address

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 in some cases provided the full 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 needed additional information for a secure identification to ensure that the complainant's personal data are not unduly disclosed. In doing so, Klarna has provided information that is counted as possible points of identification for the appellant.

Grounds for the decision

Applicable provisions, etc.

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 access³ 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 complete 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 arise as a result of 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

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.

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 Privacy Protection Authority

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 appellant?

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 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.

It appears from the complaint that, in the context of his request for erasure on 11 January 2021, the complainant provided his name. Furthermore, it appears that, on 18 January 2021, in response to Klarna's request for additional information, the applicant provided its date of birth and, at the same time, also requested access to its personal data. Klarna, on the other hand, stated that the complainant had provided her name and e-mail address and that Klarna had reasonable grounds to doubt her identity, since the complainant had provided only two out of three data points necessary for it to be regarded as identified in accordance with the current procedure. 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 processed by Klarna, and having regard to the information provided by the applicant in its request for erasure, notwithstanding the existence of different information concerning which two of the three necessary information was provided, IMY considers that there is no reason to call into question the fact that, at the time of

⁶ EDPB Guidelines 01/2022, paragraph 71.

the applicant's request of 11 and 18 January 2021, Klarna had reasonable doubts as to the identity of the applicant.

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 which personal data are requested. A proportionality assessment must be carried out in order to determine what is appropriate in the light of the requirements of the Regulation 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 must facilitate the exercise of the rights of the data subject. That assessment shall also concern whether the additional information is proportionate to the type of data processed and the harm that may result from the disclosure of data to the wrong person.

Furthermore, according to the EDPB Guidelines on the right of access, when assessing proportionality, the controller must take into account, inter alia, 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

In summary, Klarna has stated that data subjects can identify themselves through three data points established in Klarna's routine, which can be submitted in different combinations. In the present complaint, Klarna has requested three data points relating to the complainant's first and last name, date of birth, and the email address he used when purchasing through Klarna.

IMY initially considers that the requirements for identification, in terms of the nature of the personal data that Klarna processes and the negative consequences that may arise from unauthorised disclosure of the personal data, must be set relatively high.

IMY further notes that Klarna requested three data points, which, according to Klarna, is the minimum number of data points required to identify the complainant. IMY also considers that the information requested by Klarna is simpler in nature and must be regarded as readily available to the applicant in relation to the requirement laid down in Article 12(2) of the GDPR. In addition, Klarna only requests information that corresponds to information that it already processes about the complainant.

IMY considers that, in the light of the relatively high identification requirement and Klarna's indication of the number of data points required for identification, which IMY has no reason to question, the data points requested in the complaint may be considered to have been necessary to confirm the identity of the complainant.

⁷ EDPB Guidelines 01/2022, paragraph 70

IMY therefore considers that it is not apparent from the investigation in the case that Klarna requested more information than is necessary to identify the complainant in such a way that it was done in breach of Article 12(6) of the GDPR.

Has Klarna facilitated the exercise of the applicant's right of access under Article 12(2) of the GDPR?

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.

It is apparent from the complaint that, in the context of his request for erasure of 11 January 2021, the complainant provided his name. In doing so, Klarna requested the appellant to provide additional information, namely name, date of birth and e-mail address, in order to confirm the appellant's identity and subsequently deal with the appellant's request. In its reply to Klarna on 18 January 2021, the applicant provided information on its date of birth and, in connection therewith, also requested access to its personal data. From what is stated in the complaint, Klarna has again requested the same information as before, i.e. name, date of birth and e-mail address.

In IMY's view, by asking again for the same information as they had previously requested, without taking into account the information already provided by the appellant or pointing out to the appellant what information they lack in order to be able to confirm their identity, Klarna made it more difficult to exercise the appellant's rights under Article 12(2) of the GDPR.

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

Choice of intervention

In case of deficiencies, IMY may take certain corrective actions. 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 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 takes the view that Klarna has not facilitated the exercise of the appellant's rights under Article 12(2) of the GDPR. However, Klarna responded without delay to the complainant's letter in order to comply with the complainant's requests for deletion and access respectively. In addition, the applicant's request for access was satisfied on 13 August 2021. The deficiencies found are therefore less serious than if the appellant's requests had been left unanswered.

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

This decision has been made by [REDACTED], Department Lawyer

Annex

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.