COMPLAINANT
See appendix

CONTROLLER
Klarna Bank AB

Swedish ref.:
IMY-2025-8241

German ref.:
521.14108/631.344

IMI case register:
CR134712

Date:
2025-12-15

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 made on 14 January 2021 and 18 June 2021 has processed personal data in breach of:

- Article 12(6) of the GDPR[1] by requesting more data than necessary to identify the complainant for the purpose of exercising rights
- Article 12(2) of the GDPR by not facilitating the exercise of the complainant's rights
- Article 21(3) of the GDPR by not ceasing to process the complainant's data for direct marketing purposes after the complainant objected to such processing.

The Swedish Authority for Privacy Protection finds that it is not apparent from the investigation in the case that Klarna Bank AB failed to comply with Articles 32, 15(1) and 15(3) of the GDPR in the manner alleged in the complaint.

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), 12(2) and 21(3) of the GDPR.

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

[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).

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

of each complaint will take place in separate cases. The complainant at hand has lodged several complaints against Klarna regarding the same requests for the exercise of the same rights. IMY has against this background merged the complaints into one matter.

IMY's investigation of the complaint in the present case has been limited to the questions whether Klarna

- acted in accordance with Article 12(6) of the GDPR when it requested data to identify the complainant in the exercise of his rights
- facilitated the complainant's exercise of rights in accordance with Article 12(2) of the GDPR
- fulfilled the requirements for appropriate security measures under Article 32 of the GDPR in the exercise of the rights of the complainant
- acted in accordance with Articles 15(1) and 15(3) of the GDPR when the complainant requested access to his personal data
- acted in accordance with Article 21(3) of the GDPR when the complainant objected to the processing of his personal data for direct marketing purposes.

The investigation in the case concerns Klarna's handling of the complainant's requests made on 14 January 2021 and 18 June 2021. 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.

Request 14 January 2021

On 14 January 2021, the complainant received a direct marketing e-mail from Klarna despite the fact that the complainant denied to such when registering. On the same day, the complainant requested access to his personal data and objected to Klarna continuing to process his personal data for direct marketing purposes.

In the context of its request, the complainant provided the following information:

- Last name
- E-mail address.

E-mail correspondence between the complainant and Klarna shows that Klarna required the following information in order to handle his request:

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

Klarna also requested the complainant to provide a telephone number in order to send him a password and to open an encrypted copy of his personal data. Klarna also required the complainant to provide IBAN numbers in the event that the complainant has used Klarna Open Banking via a third-party provider and wants access to the personal data stored by that third-party provider.

The complainant objected to submitting additional information, arguing that Klarna does not need all the information to identify him and that Klarna should already have access to such data, given that it sends him direct marketing. The complainant also objected to sending the personal data to Klarna by unencrypted e-mail and stated that he wished his personal data to be sent to his postal address.

Klarna again requested the information in order to handle the complainant's request and stated that the complainant had the possibility to send the information by physical mail to Klarna. After some e-mail correspondence with the complainant, Klarna stated that the complainant could use the 'Unsubscribe' button in one of its e-mail marketing communications in order to prevent such further direct marketing.

Following further correspondence, the complainant sent a key to an encrypted e-mail with the requested personal data. Klarna replied that they were not able to open the data in the sent format and that they could not comply with his request if unable to identify him and that they will refrain from further contact until they have received the requested information.

Request 18 June 2021

Since Klarna did not comply with the above request and the complainant received a new direct marketing e-mail on 17 June 2021 from Klarna, the complainant sent a new request on 18 June 2021 for, inter alia, the right of access and objection to Klarna continuing to process his personal data for direct marketing purposes.

In the context of its request, the complainant stated:

- First and last name
- E-mail address.

The e-mail correspondence between the complainant and Klarna shows that Klarna required the following information in order to handle the request:

- Date of birth
- E-mail address used for purchases with Klarna
- Klarna invoice number for one of the orders
- Name of a merchant the complainant placed an order with
- Exact invoice amount for one of the orders
- Invoice address (in case the complainant has used the product Billpay).

In addition, Klarna requested the complainant to provide his old and new postal address, if he has moved within the last 24 months, for verification purposes. Klarna also requested the complainant to provide a telephone number that would be used to send a password in order for him to open an encrypted copy of the personal data. Finally, it Klarna also required the complainant to provide transaction IDs and IBANs in the event that the complainant used Klarna Open Banking via a third-party provider and access to the personal data stored with it.

The complainant subsequently sent Klarna the following information:

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

Klarna subsequently requested the same personal data from the complainant, after which the complainant questioned that Klarna continued to request information already provided by him.

Once Klarna handled the request for the right of access, the complainant did not receive all the information and Klarna also chose to send a copy of personal data digitally despite the fact that he wanted them by physical mail, which would have been a safer option.

Statement by Klarna

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

Request made 14 January 2021

By e-mail on 14 January 2021, Klarna received the complainant's request for access to his personal data, objection to having his personal data processed for direct marketing purposes and information on when the complainant gave his consent to marketing e-mails. Klarna initiated the identification process on 22 January 2021.

The complainant did provide the information required in a format that Klarna was able to open. On 10 March 2021, the complainant was informed that the case will be closed if Klarna did not receive the data necessary to complete the identification in a format that can be opened. Since the complainant did not provide such information, the request could not be met. In addition, on 15 February 2021, Klarna informed the complainant of how he himself could proceed to cancel further marketing e-mails.

Request made 18 June 2021

By e-mail on 18 June 2021, Klarna received the complainant's request for access to his personal data, objection to having his personal data processed for direct marketing purposes and information on when the complainant gave consent to marketing e-mails. Klarna initiated the identification process on 22 June 2021.

Although complainant objected to the need for all the information, he provided the requested information on 22 June 2021. The customer service employee who dealt with the case has inadvertently not noticed this and therefore again requested the information. Following the complainant's reference to the data previously provided on 3 July 2021, a copy of the complainant's personal data was sent on 26 July 2021. In this context, Klarna also provided information on when the complainant accepted the terms and conditions and the marketing communications. However, Klarna could not establish with certainty whether the marketing e-mailing were closed on 26 July 2021, in any event the request was satisfied on 23 September 2022.

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 requests, Klarna had reason to doubt the identity of the complainant, since the complainant, regarding the first request, only provided his e-mail address, and, regarding the second request, only provided his e-mail address and his name, i.e. one respectively two of the necessary data points to be considered identified according to the current routine. For this reason, Klarna has not been able to fulfil the request.

What information has Klarna required to handle the request?
Klarna states, as may be understood by the supporting documents, that the complainant was asked to provide the following information:

- Name (only for first request)
- Date of birth
- E-mail address

- Invoice number
- Name of a merchant the complainant placed an order with
- Purchase amount for invoice
- Billing address if Billpay was used (only for second request).

The complainant was also asked to provide the telephone number so that Klarna could send the complainant a password and he could open a copy of his 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 identification process 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.

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?
For identification purposes, Klarna generally and only, as may be understood, collects data corresponding to the data already collected.

What means of communication can the complainant use to confirm his or her identity and how has the complainant been informed of these possibilities?
Klarna states that it provides several means of contact to enable the complainant to confirm his or her identity. A customer can contact Klarna and identify themselves via e-mail, chat, web form, telephone and post, as can be seen from Klarna's website, which is also referred to in Klarna's data protection information and in other information that Klarna provides to its customers.

Klarna's customer service staff has informed the complainant in question of the possibility of identifying himself via physical mail as an alternative to e-mail.

Can Klarna not receive the requested data via encrypted e-mail?
Klarna applies encrypted transmission through the Transport Layer System (TLS) to prevent unauthorized access to e-mail when it is sent over internet connections. Encryption with TLS requires that both the sender's and the recipient's e-mail operator use TLS. The claim that Klarna requests data via unencrypted e-mail is therefore incorrect. Once the content has been received by Klarna, Klarna's internal security and

compliance principles for data minimization, the principle of minimum permissions and role-based access control are followed.

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 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.

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 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 controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access request 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 minimization 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

[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.

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

Pursuant to Article 32(1) of the GDPR, the controller must take appropriate technical and organisational measures to ensure an appropriate level of security for the data processed. When assessing the appropriate technical and organisational measures, the controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of natural persons.

It follows from Article 15(1) of the GDPR that the controller is obliged, at the request of the data subject, to provide confirmation as to whether or not personal data concerning him or her are processed and, if so, to provide access to personal data and to provide the data subject with additional information concerning, inter alia, the purposes of the processing and the recipients of the data. Where the data subject makes the request for access by electronic means, the information shall be provided in an electronic commonly used electronic form in accordance with Article 15(3), unless the data subject requests otherwise.

Under Article 21(2) of the GDPR, the data subject has the right to object at any time to the processing of personal data concerning him or her for the purposes of direct marketing. Furthermore, Article 21(3) of the GDPR states that the personal data may no longer be processed for such purposes if a data subject objects to the processing.

The assessment by IMY

Has Klarna acted in accordance with Article 12(6) of the GDPR when Klarna requested additional data from the complainant?

Has Klarna had reasonable grounds to doubt the identity of the complainant?
It is only where the controller has reasonable doubts as to the identity of the requester that additional information to confirm the identity may be requested. What constitutes 'reasonable grounds' in Article 12(6) of the GDPR should be assessed in the light of the circumstances of the individual case. The assessment of whether there are reasonable grounds to doubt the identity of the requester in an individual case is normally made in the light of the information provided in the context of the request. This is particularly true in situations where the controller does not have detailed knowledge of that person. However, the need for an individual assessment does not preclude the establishment of procedures by which the controller normally verifies the identity of the data subject.

The requirements that can be placed on the information should typically be higher the more sensitive the processing of the personal data is. In other words, one type of information for identification may be sufficient for identification in the case of one processing operation but may cast doubt in the case of another.

The complainant states that he provided his name and e-mail address when he sent his requests for the right of access and objection to the processing of his personal data for direct marketing purposes. He has subsequently provided additional information, as requested by Klarna, on both occasions.

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

Klarna states that, with regard to the first request, the complainant merely provided his e-mail address and Klarna was unable to open the provided additional personal data in the format sent by the complainant. Klarna had reasonable doubts as to the complainant's identity, since the complainant had provided only one of several data points necessary for it to be regarded as identified in accordance with the procedure in force at the time. As regards to the second request, the complainant merely provided his e-mail address and name and Klarna had reasonable grounds to doubt the complainant's identity, since the complainant provided only two of several data points necessary to be regarded as identified in accordance with the procedure in force at the time. Klarna has not mistakenly noted that the complainant subsequently supplemented the request before the complainant brought it to Klarna's attention, after which Klarna was able to satisfy the request.

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 had reasonable grounds to doubt the complainant's identity regarding his requests for access.

However, IMY considers that the risk of negative consequences for data subjects in the exercise of the right to object to further processing of personal data for direct marketing purposes is significantly lower than in the exercise of the right of access. According to IMY, incorrect deletion of data linked to marketing communications would not entail any major disadvantages. The requirements for identification have therefore been relatively low. It is further noted that the function of 'Unsubscribe' in an e-mail does not necessarily imply additional elements of identification of the scope required by Klarna in this case for the complainant to exercise its right and stop receiving marketing e-mail. Support documents also show that, with regards to at least the second request, the complainant sent his request to Klarna from the same e-mail address to which the marketing communication was sent to and of which Klarna also received a copy in connection with the complainant's objection to the marketing. Against this background, IMY considers that Klarna had no reason to doubt the complainant's identity with regards to his objection to the continued processing of personal data for direct marketing purposes.

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, Klarna asked the complainant to provide at least 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 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 with regards to the complainant's request for access. At the same time, IMY considered that Klarna had no reason to impose the same high identification requirements in order to handle the complainant's objection to direct marketing.

However, according to Klarna itself, not all of the additional information requested was necessary to identify the complainant in relation to the made requests. In addition, supporting documents provided by the complainant show that Klarna repeatedly requested additional information (including at least six data points) in order to handle the requests and that it also, by mistake, requested information already provided by the complainant in the context of the requests.

IMY has assessed that Klarna did not have reasonable grounds to doubt the identity of the complainant in relation to his objection to direct marketing and it can already be concluded for that reason that Klarna requested more information than was necessary to identify the complainant's identity, at least as regards that request.

Furthermore, 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 on the basis of the varying risks that existed in relation to the respective requests made

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

by the complainant. 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 and, with regards to the second request, to the repeat request further data even though the information has already been provided is contrary to the provision in question.

In view of the fact that more data than was necessary to identify the complainant in the exercise of his rights 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 certain information by e-mail in order to be able to confirm the complainant's identity and then further handle the complainant's requests. Klarna states that there are several means of contact through which data subjects can exercise their rights and supporting documents show that Klarna has informed of this when he has objected to the providing information by e-mail. Furthermore, supporting documents show that the complainant has been asked to provide information on, inter alia, the invoice number, the name of a merchant with which the complainant previously made a purchase and exact purchase amount for invoice through e-mail and this for the exercise of all rights.

As can be seen above, IMY considered that not all the information requested by Klarna was necessary to identify the complainant for the purposes of either the right to access or, in particular, the objection to the processing of personal data direct marketing purposes. As a result, the complainant had to carry out research in order to find several items of information relating, inter alia, to previous purchases, even though that information was not always necessary.

IMY therefore concludes that Klarna, by requested the complainant to provide further information that have not always been necessary for identification purposes, 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.

Has Klarna met the requirements for appropriate security measures under Article 32 of the GDPR in the exercise of the complainant's rights?
Article 32(1) of the GDPR requires the controller to take appropriate technical and organisational measures to ensure an appropriate level of security to protect the data processed.

Klarna has requested the complainant to provide certain information by e-mail in order to be able to confirm the complainant's identity and then further handle the complainant's requests. The complainant has, in addition to question the necessity of such further information, objected to submitting the requested personal data via unencrypted e-mail. The complainant has requested a secure contact route for Klarna's identification of him but also for Klarna's disclosure of his personal data.

IMY has to decide whether Klarna has ensured an appropriate level of security regarding the personal data of the complainant that Klarna has requested by e-mail to identify him and by providing a copy of his personal data through digital means.

The appropriate level of security varies according to, inter alia, the risks for the rights and freedoms of natural persons posed by the processing and the nature, scope, context and purposes of the processing. For example, the type of personal data being processed must be taken into account in the assessment.[8] Processing of sensitive and privacy-sensitive personal data requires stronger protection under the General Data Protection Regulation.

There are risks associated with using e-mail to send personal data, for example that unauthorized persons can access, spread or distort it. The level of security required must be assessed in the light of the amount of personal data being processed, for what purpose, what types of data are involved and what risks there are with the processing for the individual. However, this does not mean that e-mail always needs to be encrypted if the personal data sent via e-mail does not constitute sensitive, particularly worthy of protection or otherwise privacy-sensitive personal data.

In the present case, Klarna requested the complainant to, inter alia, provide his date of birth, e-mail address, invoice number, name of a merchant from which he had previously made a purchase and exact invoice amount. As understood by IMY, it should essentially be similar personal data when providing a copy of the personal data. IMY notes that there was thus no question of sensitive, particularly worthy of protection or otherwise privacy-sensitive personal data.

Klarna has further stated that the company uses standard encryption through Transport Layer Security (TLS) that encrypts the transmission of e-mails to ensure privacy and a secure delivery. The purpose of TLS is to prevent unauthorized access to e-mail when it is sent over an open network such as the internet. Encryption with TLS requires both the sender and the receiver to support it, otherwise the transmission is not encrypted. Klarna cannot guarantee that Klarna will be able to receive e-mails encrypted by any other encryption method.

IMY notes that Klarna has stated that it offers a certain encryption method for the transmission of e-mails. Supporting documents also show that the complainant has only objected to this with regards to his first request and that Klarna informed him of the possibility to provide the information through physical mail, something the complainant did not do. As also stated above, the requested data does not constitute sensitive, particularly worthy of protection or otherwise privacy-sensitive personal data.

In conclusion, IMY considers that the investigation shows that Klarna has not failed in its obligations to ensure an appropriate level of security with regard to these data that Klarna requested to identity the complainant nor when Klarna provided the complainant with a copy of his personal data.

IMY therefore concludes that Klarna did not process the complainant’s personal data in breach of Article 32 of the GDPR in the manner alleged in the complaint.

[8] See recitals 75 and 76 of the GDPR.

Has Klarna complied with the complainant's request for the right of access under Article 15(1) of the GDPR?
According to Article 15(1) of the GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, if so, access to the personal data and certain information.

The complaints show that the complainant requested access to his personal data on 14 January 2021 and 18 June 2021 and that he received a copy of his personal data on 26 July 2021. This is in line with the information provided by Klarna in the case. However, the complainant has also stated that his request for access has not been fully met because he has not been provided with a copy of the communication with Klarna and that Klarna has not provided all the information required by the request for access. Klarna has stated that it had met the complainant's request for access.

IMY notes that there is no evidence to support the complainant's statement that Klarna failed to comply with the complainant's request for the right of access. There is no reason to question the company's statements in this regard.

IMY therefore considers that it is not shown that Klarna has not comply with the complainant's request for the right of access under Article 15 of the GDPR.

Has Klarna met the complainant's request to receive his personal data in the form as requested in accordance with Article 15(3) of the GDPR?
Under Article 15(3) of the GDPR, the controller shall provide the data subject with a copy of the personal data undergoing processing and the data subject that makes the request in electronic form shall be provided the information in electronic form, unless the data subject requests otherwise.

The complainant states that Klarna sent a copy of his personal data by e-mail and digitally, even though he requested them by physical mail. Klarna stated that it had complied with his request for access.

IMY notes that the investigation shows that the complainant made the request for the right of access in electronic form by e-mail and that, as regards his first request, he wished to have his personal data sent to him by physical mail. However, Klarna did not comply with that request because it did not receive additional information to identify the complainant. As regards to his second request for the right of access, which was also made electronically by e-mail, IMY considers that it is not apparent from the supporting documents that the complainant stated that he wished to have his personal data sent to him by physical mail. In addition, according to the complainant's own statement, he provided Klarna with a telephone number in order for Klarna to send the security code to him and he receive the copy of the personal data digitally.

IMY therefore considers that it the investigation does not show that Klarna acted in breach of Article 15(3) when sending copies of the complainant's personal data digitally to the complainant.

Has Klarna acted in accordance with Article 21(3) of the GDPR when the complainant objected to Klarna's direct marketing?
If a data subject objects to direct marketing pursuant to Article 21(2) of the GDPR, personal data shall no longer be processed for such purposes according to Article 21(3) of the GDPR.

The investigation in the case show that the complainant received direct marketing by e-mail and subsequently objected to this processing both on 14 January 2021 and 18 June 2021. Klarna has stated that the complainant's objection to the processing of personal data for marketing purposes has not been handled. This is because at the time of the first request in January 2021, the complainant was not identified and that Klarna had not mistakenly noted the complainant's addition at the time of the second request in June 2021.

IMY has assessed that Klarna did not have reasonable grounds to doubt the complainant's identity in relation to his objection to direct marketing, at least not since he made such a request from the same e-mail as the direct marketing mailings in June 2021. However, it is clear from the investigation in the case that Klarna continued to process his personal data for direct marketing purposes after the objection and only much later, on 23 September 2022, ensured that the marketing mailings, according to the request, were cancelled.

Klarna has stated that it informed the complainant how he could stop the marketing communications himself. IMY notes, however, that Klarna has had an obligation to deal with the complainant's request as made via e-mail address. A data subject is not limited to making use of designated channels of communication, but may also request that his or her rights be safeguarded through other official channels of contact with the controller, as the complainant has done in the current case. Against this background, Klarna has had an obligation to handle the complainant's objection despite the fact that it was made by e-mail instead of referring the complainant to take further steps himself to cancel the marketing communications.

IMY therefore considers that by continuing to process the complainant's personal data for direct marketing purposes, despite the complainant having objected to such processing, Klarna acted in breach of Article 21(3) of the GDPR.

Choice of corrective measure

In case of deficiencies, IMY may take certain corrective actions. 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 for the exercise of his rights. 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 rights and has cancelled processing personal data for direct marketing purposes, even though the complainant objected to such processing. However, Klarna responded without delay to the complainant's e-mails in order to comply with his requests. Although the complainant's requests was

only granted in July 2021 respectively in September 2022, the deficiencies found are of a less serious nature than if the requests 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 made by [redacted], Department Lawyer, following a presentation by [redacted], Legal Advisor.

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.