

**Notice:** This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-01-19, no. IMY-2022-1032. Only the Swedish version of the decision is deemed authentic.

**Ref no:**  
IMY-2022-1032

**Date of decision:**  
2023-01-19

# Decision under the General Data Protection Regulation – Lensway Group AB

## Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Lensway Group AB when handling the request for erasure made on 20 February 2020 by the complainant in Complaint 1, and the request for erasure made on 25 June 2020 by the complainant in Complaint 2, has processed personal data in breach of:

- Article 12(6) GDPR<sup>1</sup> by requesting a copy of the identity document and signature when this was not necessary to confirm the identities of the complainants; and
- Article 12(2) of the GDPR by requiring that the complainants when requesting erasure submit information by mail in order to confirm their identities, which did not facilitate the exercise of the complainants' right to erasure.

The Swedish Authority for Privacy Protection issues a reprimand to Lensway Group AB pursuant to Article 58(2)(b) of the GDPR for infringement of Articles 12(2) and 12(6) of the GDPR.

## Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Lensway Group AB (the company) due to two complaints, mainly to investigate whether Lensway Group AB has received and handled the complainants' requests for erasure in accordance with Articles 12 and 17 of the GDPR. The complaints have been submitted to IMY as the lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made by the supervisory authority of the country where the complainants have lodged their complaints (Finland and Denmark) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

**Postal address:**  
Box 8114  
104 20 Stockholm

**Website:**  
[www.imy.se](http://www.imy.se)

**E-mail:**  
[imy@imy.se](mailto:imy@imy.se)

**Phone:**  
08-657 61 00

The case has been handled through written procedure. In view of the complaint relating to cross-border processing, IMY has made use of the cooperation and

<sup>1</sup> 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).

consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Norway and Finland.

### **The complaints**

The complainants have mainly stated the following.

#### *Complaint 1 (Complaint from Finland with national registration number 1576/153/2020)*

The complainant was in contact with the company on 20 February 2020 and requested erasure. The company replied to the complainant that the complainant needs to send them the postal address so that they can send the complainant documents relating to the complainant's request. These documents were to be signed and returned by the complainant. In addition, the company requested the complainant to verify the identity by sending a copy of the complainant's identity document by e-mail. For security reasons, the complainant was not willing to provide what was requested.

#### *Complaint 2 (Complaint from Denmark with national registration number 2020-31-3616)*

The complainant requested erasure of the complainant's information on lensway.dk. In order to comply with the request, the company requested that the complainant provide the social security number and a copy of the identity document. However, the company could not tell the complainant why they need that information except that they need it in order to confirm the complainant's identity. The complainant questions the need for the company to collect personal data in order to erase personal data. The complainant suggested that the company could instead confirm the complainant's identity by sending an e-mail to the address registered on the complainant but they refused.

### **What Lensway Group AB has stated**

In its statements of 20 April, 12 May and 11 August 2022, the company has mainly stated the following. The Company is the data controller concerning the processing to which the complaints relates.

#### *Complaint 1*

The company has received the complainant's request for erasure, but the complainant has not completed the company's at the time current verification process. The company has requested the complainant to submit a copy of the identity document. This is the only way the company has so far been able to ensure the identity of the customer. The copy was to be sent by regular mail. The company also requested the complainant to submit a signed request for erasure. The company has so far not been able to receive this information digitally. In order to ensure that they have received original documents, they have asked the complainant to submit it via regular mail.

#### *Complaint 2*

The company received the request for erasure on 25 June 2020 but the complainant did not complete the company's at the time current verification process. It is true that the company requested the complainant's social security number in the written form, but it has been voluntary to provide this information. In addition to the information requested in the written form, the company requested the complainant to submit a

copy of the identity document. The company has so far not been able to identify the complainant in any other way. The complainant was asked to submit the information by regular mail in order to ensure that the company had received the original documents.

*As regards both complaints the company has stated the following:*

As regards the written form to be submitted by both complainants, the company states the following concerning the personal data required to disclose and why the information was necessary.

- Name is mandatory information which is requested to confirm the identity of the data subject.
- Email address is mandatory information which is requested because it is used as a unique identifier of customers in the company's system.
- Signature is mandatory for the company to be able to ensure that the data subject has read the information and has given his or her consent.

The company states that they should always ensure that it is the right person that contacts them when it comes to requests to exercise a right under the GDPR. Since the company was previously unable to identify the customer in a good and secure way when they contacted the company through customer service, the manual process via regular mail has been the one they have used. In this way, they have had a two-step verification. Functionality to enable confirmation of the customer's identity through customer service has not been in place.

The customer relationship with the company can be established in two ways, either the customer makes a purchase or the customer logs in to My Pages. When the customer creates an account on My Pages, the customer enters their email address and an email with confirmation is sent to the customer. The customer can then, via the link in the email, come to a web page where they link a password to the email address. The customer account is then created and the company thus receives a two-step verification. The complainants used the second method by which the customer relationship can be established.

The complainants made purchases with the company and they were identified through the company's payment service provided by Klarna. For most payment options, Klarna requires the customer to verify themselves via bank ID. For certain payment methods, for example payment by credit card, the customer may choose not to have to verify via bank ID through Klarna's app.

The company's existing digital contact channel is My Pages. However, there has been no functionality to handle requests to exercise a right under the GDPR on My Pages. Since April 2022, the company's customers can now request to be erased or receive a copy of their personal data directly via My Pages. The customer's identity is then verified via regular login.

## Statement of reasons for the decision

### Applicable provisions, etc.

According to Article 17(1), the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds set out in the Article applies, for example when the personal data are no longer necessary in relation to the purposes for which they were collected or if the data subject withdraws consent on which the processing is based.

Article 12(2) requires the controller to facilitate the exercise of data subject rights under Articles 15 to 22.

Article 12(6) states that, without prejudice to Article 11, 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's (EDPB) Guidelines 01/2022 on access<sup>2</sup> state inter alia:

65. In cases where the controller requests the commission of 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 (see section 3.3). Such additional information should not be more than the information initially needed for the verification of the data subject's identity (authentication). In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which is not relevant or necessary to strengthen the link between the individual and the personal data requested.

[...]

73. It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate, unless it is strictly necessary, suitable, and in line with national law. In such cases the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.

---

<sup>2</sup> EDPB, Guidelines 01/2022 on data subject rights — Right of access, Version 1.0. The guidelines have been out for public consultation and are awaiting final adoption.

## Assessment of IMY

On the basis of the complaints in question, IMY has examined the company's conduct in these two individual cases.

### **Has the company acted in accordance with 12(6) of the General Data Protection Regulation when the company requested current information from the complainants?**

*Has Lensway Group had reasonable grounds to doubt the identity of the complainants?*

It is only when the controller has reasonable grounds to doubt the identity of the person making the request that additional information to confirm the identity may be requested. What constitutes "reasonable grounds" in Article 12(6) GDPR should be assessed on the basis of the circumstances in the individual case. The assessment of whether there are reasonable grounds in an individual case to doubt the identity of the one requesting is normally made in the light of the information provided in connection with the request. This applies particularly in situations where the controller has no further knowledge of the person. However, the need for an individual assessment does not preclude the establishment of routines for how the controller normally verifies the identity of the data subject.

The company was given the opportunity to motivate the individual assessment made based on the complainants' situation if they considered that they had reasonable doubts as to the identity of the complainants when the complainants submitted their requests. With regard to both complainants, the company argues mainly as follows. The company should always ensure that it is the right person that contact them when it comes to requests to exercise a right under the GDPR. The customer has not previously been able to be identified in a good and secure manner when they contacted the company through Customer Service. Functionality for handling requests to exercise a right under the GDPR has not been available through Customer Service or on My Pages.

IMY notes that it is not clear from the investigation in the case what information the complainants provided in connection with their request and whether there were reasons for the company to doubt their identity on the basis of those requests. However, IMY considers that, in light of what has emerged in the case, there is no need to question the company's statement that it had reason to doubt the identity of the complainants. In the assessment, IMY takes into consideration the fact that the obligation to ensure the identity of the one requesting also is intended to protect data subjects against someone else making requests in their name, which may lead to negative consequences for the data subject. The risks of these negative consequences in the event of false requests are particularly obvious in the case of more invasive measures, such as the exercise of the right to erasure. IMY therefore takes the view that it has not been shown other than that the company, in the present cases, have had reasonable grounds to doubt the identity of the complainants.

*Has the information requested by the Lensway Group been necessary to confirm the identity of the complainants?*

Although the controller has reasonable grounds to doubt the identity of the data subjects, the controller shall not collect more personal data than is necessary to enable the confirmation of the identity of the requesting data subject.

The company mainly states the following concerning the necessity of the information they have requested from both complainants. A copy of the identity document has been requested as it was the only way in which the company has so far been able to verify the identity of the customer. In addition to a copy of the identity document, the complainants were required to submit a written form. The information requested in the written form and why it was necessary is presented by the company in essence as follows. The name has been requested to confirm the identity of the data subject. The email address has been requested because it is used as a unique identifier of customers in the company's system. The signature has also been requested and is, according to the company, a necessary information for the company to be able to ensure that the data subject has read the information and given his or her consent to the handling of the request.

As regards the verification of the identity of the complainants, the company states that both complainants made purchases where they were identified through the company's payment service provided by Klarna.

It appears from the company's statements that it was not required that the company itself verified the identity of the complainants when the customer relationship was established, i.e. at the time of purchase. IMY states that the company cannot require more personal data when the complainant wishes to exercise its rights than was required when establishing the customer relationship. A copy of the identity document and signature is information that the company has not requested at the establishment of the customer relationship in these two cases. Furthermore, IMY takes into account that, according to the EDPB Guidelines on the right of access, the use of a copy of an identity document as part of the authentication process should be considered inappropriate, unless strictly necessary, suitable and in line with national law. IMY considers that the requirement to provide the controller with a copy of its identity document is an intrusive measure, which is only appropriate where the controller has previously ensured the actual identity of the data subject and where alternative less intrusive means of verification are inappropriate. IMY considers that there have been no circumstances identified that speak against that other, less intrusive, verification methods could have been used in the present cases, such as login via My Pages or control questions. IMY notes that it has therefore not appeared in the case that the request for a copy of the identity document or the signature would have been absolutely necessary or appropriate.

Against this background, IMY considers that the copy of the identity document and the signature cannot therefore be considered to have been necessary to confirm the identity of the complainants in accordance with Article 12(6) of the GDPR.

**Has the company acted in accordance with 12(2) of the General Data Protection Regulation when the company requested the complainants to send the information by mail?**

The next question is whether it has been permissible to require the complainants to send the requested information to the company by regular mail.

In view of the requirements to facilitate the exercise of the data subject's rights in Article 12(2) GDPR, it can only be accepted in exceptional cases that a controller as the sole channel of contact refers individuals to ordinary mail if they have to submit information in order to ensure their identities, for example if it is justifiable for reasons of security. The starting point should be that alternative means of submitting requested information should be offered. In that regard, the company has mainly stated that it required the information to be sent by regular mail in order to ensure that they received the original written documentation.

IMY takes the view that the transmission of a copy of an identity document may indeed pose particular risks, which may justify requiring that the document be sent by mail. This provided that it is necessary information to confirm the identity of the data subject.

In the present cases, IMY concludes above that a copy of the identity document was not necessary to confirm the identity of the complainants. By requiring the complainants additionally to send the information by regular mail, IMY takes the view that the company did not facilitate for the complainants to exercise their right to erasure. IMY therefore considers that the company thereby acted in breach of Article 12(2) of the GDPR.

#### **Choice of corrective measure**

It follows from Article 58(2)(i) 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 in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be taken into account when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. It has emerged from the investigation in the case that a copy of an identity document and signature is no longer requested by Lensway Group AB upon requests from data subjects to exercise their right to erasure under the GDPR. Furthermore, the infringements found have occurred relatively far back in time (2020) and have affected two data subjects. Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that Lensway Group AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

---

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED], following a presentation by legal advisor [REDACTED]

## How to appeal

If you wish to appeal IMY:s decision, please write to IMY. Please indicate in your letter the decision you are appealing and the amendment that you are requesting. The appeal must reach IMY no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, IMY forwards it to the Administrative Court in Stockholm for trial.

You can send the appeal by email to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. IMY:s contact details are set out in the first page of the decision.