Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision 2021-12-17, no. DI-2020-10525. Only the Swedish version of the decision is deemed authentic.

Ref no:
2020-10525
IMI case no. 101348

Date of decision:
2022-02-16

Date of translation:
2022-02-17

Supervision under the General Data Protection Regulation – Nordnet Bank AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Nordnet Bank AB has has processed personal data in breach of Article 12(2) of the General Data Protection Regulation (GDPR)[1] by requiring the complainants, in complaint 1 and 2, to submit data in order to prove their identities via regular mail, even though Nordnet Bank AB had a digital service (communication centre) for other customer communications that require identification. Nordnet Bank AB has thus not sufficiently facilitated the exercise of the data subjects' rights.

The Swedish Authority for Privacy Protection issues Nordnet Bank AB a reprimand in accordance with Article 58(2)(b) for the infringement of Article 12(2) of the GDPR.

Report on the supervisory matter

The procedure

The Authority for Privacy Protection (IMY) has initiated supervision regarding Nordnet Bank AB (Nordnet or the company) due to two complaints. The complaints has been submitted to IMY, as responsible supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Finland) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of complaints relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Norway, and Finland.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
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 he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

What is stated in the Complaints

Complaint 1 (Finland with national registration number 2188/182/18)

The complainant contacted the company on 25 May 2018 regarding a request for access. The company required the complainant to send the request by e-mail with a copy of their ID document, which means that the copy may need to be signed and scanned. The complainant is of the view that Nordnet hinders the exercise of the right of access and refuses to act upon a request.

Complaint 2 (Finland with national registration number 3251/182/18)

The complainant has filed a complaint to the Finnish Data Protection Authority on 14 June 2018 after contacting the company regarding a request for access. Nordnet required the complainant to submit a signed request in writing together with a copy of a valid identification document. The company denied the complainant to use the web service for exercising the right of access. It is further stated that the company's web service already has high requirements for identification as it is a business in the financial sector. The complainant wonders whether the company can refrain from acting on a request for access that is attached and sent via its web service and argues that the company makes the exercise of the right of access more difficult.

What Nordnet Bank AB has stated

Nordnet Bank AB has essentially stated the following. Nordnet Bank AB is the data controller for the processing operations to which the complaint relates.

To be able to exercise the right of access the complainants were required to use regular mail (i.e. as opposed to digital ways of communications) to submit the following data; date, place, name, signature and a certified ID copy. The company needed the information to be able to identify the data subject to whom the request relates (name and ID copy respectively), to be able to determine when the request has been made (date), and to ensure that it is the data subject himself who is exercising the right of access (signature and ID copy respectively).

As a bank, Nordnet needs to apply strict rules on identification, inter alia because of the statutory banking secrecy which means that the company may not disclose or hand out information about a customer or a customer relationship to anyone other than the customer itself.

At the time of the complaints, Nordnet referred to special forms available on the company's website. The data subjects were asked to fill in the form and attach a certified ID copy and send the documents to the company by post. The company is of the view that the complainant's statement that the request of access should be made by e-mail is incorrect.

When the company carried out a control activity, the Data Protection Officer noted that the existing procedures regarding the right to access by data subjects and to receive a copy of their data should be harmonised with how other communications with customers are handled, and thus be able to be received through the company's online customer service in line with the majority of other customer communications that require identification. New procedures for digital management of the data subject right to access the personal data were implemented accordingly in February 2020 and

requests are now received through the company's online customer service in line with other customer communications that require identification. The change makes it easier for customers to exercise their rights under the GDPR.

Justification of the decision

Applicable provisions, etc.

According to Article 5(1)(c) GDPR, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

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

Article 12(2) requires the controller to facilitate the exercise of the data subject's rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

Article 12(6) provides that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The assessment of the Swedish Authority for Privacy Protection (IMY)

On the basis of the complaints in this case, IMY examined the company's conduct in these individual cases. Therefore, IMY will not consider whether the company's current procedure for processing requests is compatible with the GDPR, but may take into account possible improvements when considering choice of corrective measures.

General starting points

It can be concluded that, in order to identify a data subject, the controller may request additional information that is necessary, where the controller has reasonable grounds to doubt the identity of the person making the request.

The GDPR does not explicitly regulate what data may be requested or how the additional information is to be collected. The controller must carry out a proportionality assessment in order to determine what is appropriate with regard to the Regulation's requirements, inter alia, for security reason, but also in the light of the requirement in Article 12(2) GDPR, according to which the controller shall facilitate the exercise of the data subject's rights. IMY finds that, requiring data on a general basis for identification purposes irrespective of whether the data is necessary as described in Article 12(6) is

contrary to both this provision and also to the principle of data minimisation in Article 5(1)(c).

A copy of the ID document should not be requested unless it´s necessary. It is only in cases where the actual identity is crucial that it could be relevant. Identification with an ID document is not necessary if the controller has not verified the correct identity of the data subject when the customer relationship was established. This means that if the controller has found it satisfactory that a customer has provided, for example, an e-mail address that does not contain the correct name when the customer's relationship was established, the controller should not require more personal data when the customer wants to exercise his or her rights.

In the light of the requirements of Article 12(2), it is only in exceptional cases acceptable for a controller to refer individuals to regular mail service as the sole route of contact when they are required to submit data in order to ensure their identities, for example if it is justifiable for security reasons. The outset should be that alternative means of submitting requested information should be offered. For example, if the controller already has digital contact service for customers that involves verification — as many controllers have for example, customer portals, messaging centres or so-called "My pages" etc. for other customer communications — it may be questioned why data subjects should be faced with a more cumbersome handling when exercising their rights under the GDPR without specific justification.

Has there been an infringement of the GDPR?

The question is whether the information required by the company — a signed request containing the date/place, name, and a certified copy of the identity document — was necessary to identify the respective complainant and whether the procedure for submitting the information offered by the company was in accordance with the GDPR.

Nordnet has been given the opportunity to justify the necessity of all the required personal data at issue and the reasons why the processing of the requests, including referring data subjects exclusively to regular mail, was justified in the present case. In summary, the company states that, as a bank, it needs to apply strict identification rules in order not to risk breaching banking secrecy laws. As regards to the handling of the data subjects' requests, the company states that, as the practice has evolved and interpretations were communicated by various European Supervisory Authorities, it has developed digital management when it comes to data subjects access to personal data, without further justifying the handling at the time of the cases in question.

In order to assess whether the information requested by the company for identification in respect of complaints 1 and 2 was necessary, account must be taken of the fact that the importance of secure identification is particularly important when individuals, as in the case, turn to a bank with a request for access. In addition, it must also be taken account, that under legislation on prevention of money laundering and terrorist financing, Nordnet is obliged to identify their customers and verify their identities when establishing customer relationship. Against this background, and the relatively small amount of personal data including the ID copy, the requested data cannot be considered unjustified. Nordnet Bank AB has therefore not violated Article 5(1)(c) or Article 12(6) of the GDPR.

However, IMY finds that, there has been no evidence which makes it justifiable to require the complainants to send the requested information to the company by regular

mail. In an overall assessment of all the circumstances, including that at the time of the complaints the company had a digital service through a messaging centre for other customer communications with identification requirements, IMY considers that Nordnet Bank AB acted in breach of Article 12(2) of the GDPR by requiring the data subjects to use regular mail to submit the required data to the company when exercising the right of access.

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) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The company have taken measures for digital management of the data subject right to access and the infringement found occurred relatively long ago and affected two individuals. Furthermore, the company has not previously received any corrective measures for infringements of the data protection rules. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Nordnet Bank AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been made by the specially appointed decision-maker [redacted] after presentation by legal advisor [redacted].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority’s contact information is shown in the first page of the decision.