

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) final decision 2022-07-18, no. DI-2021-5301. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-5301, IMI case no.
115747

Date of final decision:
2022-07-18

Date of translation:
2022-07-19

Final decision under the General Data Protection Regulation – Scandinavian Airlines System Denmark-Norway-Sweden

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that Scandinavian Airlines System Denmark -Norway-Sweden has, in relation to complaint 1, processed the complainant's personal data in breach of Article 15 GDPR¹ by not giving the complainant access to their personal data and supplementary information.

The Swedish Authority for Privacy Protection finds that Scandinavian Airlines System Denmark -Norway-Sweden has, in relation to complaint 2, processed the complainant's personal data in breach of Article 12(4) of the GDPR by not informing the complainant, without undue delay, that their personal data are not being processed.

The Swedish Authority for Privacy Protection issues Scandinavian Airlines System Denmark-Norway-Sweden a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 12(4) and 15.

Pursuant to Article 58(2)(c) of the GDPR, IMY orders Scandinavian Airlines System Denmark-Norway-Sweden, in relation to complaint 1, to comply with the complainant's request to exercise their right of access under Article 15, with exception for information which is subject to any applicable derogation provided for in Article 15(4). This is done by providing all personal data that Scandinavian Airlines processes about the complainant by providing the complainant with a copy of the personal data referred to in Article 15(3) and providing information pursuant to point (a) to (h) of Article 15(1) and information pursuant to Article 15(2). The measures shall be implemented no later than two weeks after the decision has become final

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

¹Regulation (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).

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Scandinavian Airlines System Denmark -Norway-Sweden (SAS or the company) due to two complaints. The complaints have been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authorities of the countries where the complainants have lodged their complaints (Norway and 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 a complaint 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 Norway, Finland, France, Germany, Denmark, The Netherlands, Italy, Spain and Portugal.

The complaints

Complaint 1 (from Norway with national reference number: 18/02229)

The complaint states the following. In connection with a flight from Norway to the United States with SAS on 4 July 2018, the complainant was subjected to extensive security checks both at the airport in Norway and in the United States. The complainant contacted SAS in order to obtaining information about what personal data was transferred to the US authorities in order to trigger those extra security checks. The complainant received a reply from SAS on 15 August 2018 that stated that SAS is not responsible for the additional security checks and that they were decided by US authorities. The complainant was not informed about what personal data were transferred and why. In the complaint, the complainant asks for assistance in accessing information about the transfer of their personal data to U.S. authorities as well as the personal data disclosed.

Complaint 2 (from Finland with national reference number: 6134/152/2020)

The complaint states the following. The complainant requested access to their personal data by using the company's contact form. Although 30 days have passed, the complainant has not received any confirmation that the request has been received or any response to the request.

What SAS has stated

SAS has mainly stated the following. SAS is the data controller for the processing to which the complaints relates.

Complaint 1 (from Norway with national reference number: 18/02229)

The company has received e-mail from the complainant but states that it has failed to understand the nature of the case. As a result, the complainant's request was not dealt with as an integrity request due to an oversight. The complainant has not received any information other than that set out in the annexes to the supervisory letter and has therefore not been provided information in accordance with Article 15 of the GDPR.

Since the complainant's case has not been handled as an integrity case, the company has deleted the correspondence with the complainant. The company deletes e-mails

received by customer service after 24 months. The company cannot therefore go back and see the dialogue with the complainant.

Complaint 2 (from Finland with national reference number: 6134/152/2020)

The company received the complainant's request on 5 July 2021 and finalised the case on the same day. The company offers data subjects the possibility to order a copy of their personal data through a form on the company's webpage. After ordering, SAS sends a confirmation to the customer that the order has been received, and as soon as the system has completed the extract, it is sent to the data subject by encrypted e-mail. In case the applicant's personal data are not processed, the applicant receives information about that. In the present case, no e-mail was sent to the complainant stating that their personal data are not in the system. According to the company, a system investigation is ongoing with the aim to clarify why an e-mail was not sent to the complainant and to ensure that the error does not persist. The company intends to inform the complainant when the system error has been investigated.

Justification of the decision

Applicable provisions, etc.

According to Article 5(2) of the GDPR data subjects' personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Article 29 Guidelines on Transparency, adopted by the European Data Protection Board (EDPB), state that when controllers respect the principle of transparency, data subjects can hold controllers and processors accountable and exercise control over their personal data by, for example providing or withdrawing informed consent and actioning their data subject rights.²

According to Article 5(2), the controller must always be able to demonstrate that the personal data are processed in a transparent manner vis-à-vis the data subject. In this context, the principle of liability requires the processing of personal data to be transparent towards the subject, so that controllers can demonstrate that they are complying with their obligations under the GDPR.

To anyone who requests a data controller is obliged to provide information about whether or not their personal data is being processed. If such data is processed, the controller shall, in accordance with Article 15 of the General Data Protection Regulation, provide the data subject with supplementary information and a copy of the personal data processed by the controller.

It follows from Article 15(1) what additional information is to be provided to the data subject. Article 15(1)(c) provides that the data subject shall be informed of the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries.

² Article 29 Working Party Guidelines on transparency under Regulation 2016/679 – WP260, para 4.

According to recital 63, the data subject should have the right of access to personal data processed in order to be aware that processing is taking place and verify the lawfulness of the processing.³

In the EDPB Guidelines 01/2022 on data subjects' rights — Right of access the following is stated:

“...the purpose of the right of access is to make it possible for the data subject to understand how their personal data is being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. In other words, the purpose of the right of access is to provide the individual with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).⁴

“The assessment of the data being processed shall reflect as close as possible the situation when the controller receives the request and the response should cover all data available at that point in time. This means that the controller has to try to find out about all the data processing activities relating to the data subject without undue delay.”⁵

The GDPR does not regulate the form in which a request for access is to be made. However, it is generally sufficient for a data subject to express their wish to obtain access to personal data processed or that they wish to have access to information about themselves held by the controller for a request to be regarded as a request for access within the meaning of Article 15.⁶

According to Article 12(3), a request for access must be handled without undue delay and in any event no later than one month after the request has been received. The time limit of one month may be extended by an additional two months if the request is particularly complicated or the number of requests received is high.

If the period of one month is extended, the controller must notify the data subject of the extension. The notification of the extension of the time limit shall take place within one month of receipt of the request. The controller must also specify the reasons for the delay.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy pursuant to Article 12(4) of the GDPR.

Assessment of the Authority for Privacy Protection (IMY)

Has there been a breach of the GDPR?

³ See Judgement of 7 May 2009, Rijkeboer, C-533/07, EU:C:2009:293, paragraph 50-54.

⁴ Guidelines 01/2022 on data subject rights - Right of access, adopted for public consultation 18 January 2022, para 10.

⁵ Guidelines 01/2022 on data subject rights - Right of access, para 37.

⁶ See Guidelines 01/2022 on data subject rights - Right of access, para 50.

Complaint 1 (from Norway with national reference number: 18/02229)

Regarding the first complaint, IMY finds that the complainant has contacted SAS with a request to obtaining information on how the company handled its personal data in connection with the trip to the United States. The company has stated that it has failed to understand the complainant's request as a privacy case and thus has not given the complainant access to its personal data and supplementary information in accordance with Article 15 of the GDPR, which IMY finds no reason to question. The company has thus infringed Article 15.

Complaint 2 (from Finland with national reference number: 6134/152/2020)

Regarding the second complaint, IMY finds that the complainant has not been informed that their personal data was not processed by the company in accordance with Article 12(4) of the GDPR. The company has thus infringed Article 12(4).

Choice of corrective measure

It follows from Article 58(2)(i) 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 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 infringements have affected two data subjects and the data in question was not special category data. The company states that it is carrying out a technical investigation in order to confirm why a confirmation e-mail was not sent and when that is done the company intends to inform the complainant.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Scandinavian Airlines must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

In regard to complaint 1, the company has not handled the complainant's request for access even though the company is obliged to do so. IMY therefore considers that there is reason to order the company to comply, in accordance with Article 58(2)(c), with the complainant's request to exercise its right of access under Article 15. With exception for information which is subject to any applicable derogation provided for in Article 15(4). This is done by providing the complainant access to all personal data that SAS process regarding the complainant by providing a copy to the complainant of the personal data as stipulated in Article 15(3) and provide information pursuant to points (a) to (h) of Article 15(1) and provide information pursuant to Article 15(2). The measures shall be implemented no later than two weeks after this decision has become final.

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.