Datatilsynet

NORWEGIAN AIR SHUTTLE ASA
Postboks 115
1330 FORNEBU

Your reference	Our reference	Date
	20/02288-43	16.09.2024

Decision to issue a reprimand – Norwegian Air Shuttle ASA

1. Introduction and Summary

The Norwegian Data Protection Authority (hereinafter "**Datatilsynet**", "**we**", "**us**", "**our**") is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation ("**GDPR**")[1] with respect to Norway.

We received a complaint against Norwegian Air Shuttle ASA (hereinafter "**NAS**", "**you**", "**your**"). The complaint concerned alleged infringements of facilitating data subject rights committed by NAS, in particular in connection with the verification of data subjects pursuant to Article 12.

After having investigated the complaint, we are of the view that NAS infringed Articles 12(2), 12(6) and 5(1)(c) GDPR.

2. Datatilsynet's Decision

Pursuant to Article 58(2)(b) GDPR, we hereby adopt the following decision:

Datatilsynet issues Norwegian Air Shuttle ASA with a reprimand for:

- *Infringing Article 12(6) GDPR by requesting the provision of the complainant's photo ID without demonstrating that it had reasonable doubts as to the identity of the complainant*
- *Infringing Article 5(1)(c) GDPR by requesting more information than was necessary in order to confirm the identity of the data subject*

[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) OJ [2016] L 119/1.

- *Infringing Article 12(2) GDPR by effectively imposing unnecessarily burdensome measures on the complainant by requiring provision of photo ID in order to carry out the complainant's request*

We are competent to issue corrective measures pursuant to Article 58(2) GDPR.

3. Factual Background

On 26 September 2018, we received (via the Finnish Data Protection Authority) a complaint from a data subject in Finland (the "**complainant**") against NAS in relation to NAS' processing of the complainant's personal data.

The complainant was a customer of NAS who had received a marketing e-mail from NAS on 22 May 2018. On 25 May 2018, the complainant contacted NAS through an online channel and asked NAS for a full statement of all the records it has of the complainant and why, and for clarification as to how the complainant can remove this information from NAS' records.

NAS responded on 11 June 2018 from the e-mail address "data.protection@norwegian.com" stating that in order for NAS to reply to the complainant's request it must obtain additional information from the complainant in order to verify the complainant's identity, and requested the complainant to upload a copy of their valid identification document containing their photo ("**Photo ID**") by using a link to NAS' online form.

On 18 June 2018, the complainant sent a complaint to the Finnish Data Protection Authority questioning whether NAS had the right to request a copy of their passport before fulfilling their access request (the "**Complaint**").

On 11 October 2018, we sent an order to provide information to NAS based on the Complaint, specifically aimed at the appropriateness and necessity of NAS requesting data subjects for a copy of their Photo ID in order to verify the identity of the data subject making a request.

On 7 November 2018, NAS responded to our order to provide information dated 11 October 2018 and stated, amongst other things, that it:

- processes a number of different categories of personal information and for varying lengths of time, referring to its privacy policy then applicable.
- does not require that a data subject identifies themselves in order to manage a data subject's consents.
- carried out a risk assessment in order to secure compliance with applicable data protection laws, taking into account amongst other things:
    - it processes the personal data of approximately 45 million customers,
    - many e-mail addresses do not contain a specific name,
    - the owner of e-mail addresses may change over time, and
    - many trips are ordered by persons other than those who will travel.

- therefore considers e-mail addresses themselves as not sufficient to confirm the identity of a data subject.
- considers that a copy of accepted identification documents as the best possible verification of a data subject, and if NAS are still unable to identify the data subject or there are duplicate findings, it requests further information such as last trip travelled etc.
- considers that the consequences of disclosing a data subject's personal data to an incorrect person is more severe than the burden of requesting additional information.

On 11 April 2019, NAS had a physical meeting with us to discuss the contents of NAS' response to our order to provide information and potential solutions. Further to such meeting, NAS sent an e-mail to us on 21 May 2019 stating that NAS had assessed the issue and sees that it is unfortunate that additional information is collected to allow individuals to exercise their rights under the GDPR, even though NAS considers it is important to ensure personal data is not sent to the wrong person. NAS further stated that they consider it is important that approved identification documents showing the data subject's name is shown, and proposed a potential solution where individuals could redact all superfluous information (such as the picture and social security number) from the copy of their identification document before submitting it to NAS.

On 20 June 2019, we circulated a draft decision to the other supervisory authorities concerned pursuant to Article 60(3) GDPR and proposed to close the matter without further action being taken on the condition that NAS carry out their proposed solution as outlined above and explain or give examples to data subjects as to how they may redact their approved identification document. A number of supervisory authorities concerned disagreed with such draft decision by raising objections or comments. The objections and comments of supervisory authorities concerned were summarised in a letter to NAS dated 30 April 2021 as follows:

- Controllers may not impose unnecessary or excessive procedural burdens on data subjects that wish to exercise their rights under the GDPR, and shall instead make it as easy as possible for data subjects to exercise their rights under the GDPR.

The reasoning for such disagreement was summarised in a letter to NAS dated 30 April 2021, and we ordered NAS to provide further information by answering the following questions (translated from the original Norwegian text):

1. *Do you carry out an individual assessment regarding whether there exists reasonable doubt as to the identity of the data subject that wishes to exercise their rights pursuant to Article 15-21* [GDPR]*? If so, we request that you attach your routines for this assessment.*
2. *Do you carry out an individual assessment regarding what additional information which is required to confirm the identity of the data subject? If so, we request that you attach your routines for this assessment and how this occurs in practice.*
3. *Regarding the requirement to provide a copy of a passport:*

    a. *Do you still require a copy of an identification document to confirm the identity of those that wish to exercise their rights, including those that wish to be removed from a newsletter?*
    b. *If so, have you implemented the change you proposed in the meeting of 11 April 2019, including the solution where individuals redact all superfluous information in the approved identification document*
    c. *If the provision of a copy of a passport is necessary for all data subjects that wish to exercise their rights, how do you assess this as against Article 5(1)(c)* [GDPR]*?*
4. *Facilitation of the exercise of data subject rights:*
    a. *We request that you explain in more detail how you facilitate data subjects' ability to exercise their rights pursuant to Articles 15-21* [GDPR]*, pursuant to Article 12(2)* [GDPR].
    b. *We request that you explain and attach screenshots of the "flow" on your website so that we see how the system looks from the data subject's perspective. We request that you also explain if the "flow" is the same for the exercise of all rights or if it is differentiated.*

On 11 June 2021, NAS responded to our order to provide information dated 30 April 2021 stating that it:

- updated its routines after meeting with us on 11 April 2019 to inform data subjects that they may redact all information except their name and the issuer from a copy of their valid identification document. NAS also acknowledged the need to differentiate between different types of data subject requests as, for example, wrongfully sharing personal data to those other than the data subject is not applicable to erasure requests.
- now has different routines for different types of data subject requests, namely:
    - In relation to access requests, NAS requests data subjects to provide a copy of their valid identification document but informs data subjects that they may redact all information save for their name and the name of the issuer of the valid identification document. Furthermore, if the data subject is not comfortable providing NAS with a copy of their valid identification document, NAS uses e-mail address to verify data subjects and limits the access provided to only personal data connected to the applicable e-mail address. NAS may also provide information based solely on a data subject's travel reference information.
    - In relation to erasure requests, NAS requests the data subject's e-mail address and conducts the erasure based on this. If in doubt, NAS' customer care may request additional information from the data subject such as travel reference information.
    - In relation to correction requests, NAS requests the data subject's e-mail address or travel reference information.
    - In relation to objection requests, NAS' data protection officer handles these and the verification of the data subject is based on an individual assessment.
    - In relation to newsletter requests, this is handled without verification.

- does not carry out an individual assessment as to whether a name or e-mail enables identification due to the number of requests received and the numerous possibilities related to both names and e-mails, particularly as there may be several people with the same name and many e-mails do not contain any names but often abbreviations. NAS does however carry out an individual assessment based on what the customer is comfortable sharing.
- shared copies of screenshots showing the "flow" as referenced in our order to provide information. For access requests, the screenshot shows that NAS requires the data subject to upload a copy of a valid identification document in order to identify the data subject, and states all information except the name and issuer may be redacted.

On 22 June 2021, NAS provided us with further information stating it:

- only requests a copy of a redacted valid identification document for data subject access requests.
- has initiated several GDPR projects:
    - The right to be forgotten project to ensure compliance with the requirements of Article 17 GDPR. This involves allowing the data subject to order erasure of their own data online without the involvement of NAS' customer care centre. The data subject is identified either through them logging on to their online account or through e-mail verification, potentially also with further verification e.g. by text message.
    - Consent management (marketing activities and newsletter) is handled through an online based e-mail form or the data subject's online account.
    - The access project, which will implement a new solution enabling data subjects to automatically order and receive a copy of their personal data – although noting that the verification method to be used is not yet finalised although verification could take place e.g. through text message.

On 20 August 2021, we ordered NAS to provide further information by answering the following questions (translated from the original Norwegian text):

1. *We request that you explain in more detail the ongoing GDPR activities relating to the identification of data subjects, including which changes are proposed in the on-going "GDPR projects" (in addition to that which is contained in your letter of 21 June 2021).*
2. *In an e-mail dated 21 June 2021, Linda Methlie writes:*
    a. *A data subject can delete all information on their ID except issuer and name. This solution acv id* [sic] *will be replaced by a new solution which will use another method to verify the data subject (e.g. sms). Other data subject rights pursuant to the GDPR are handled without requiring ID.*

   Does this mean that the solution requiring providing ID will be discontinued and replaced by a new solution? If so, we request you explain in more detail this solution. If the new solution involves changes to how you assess whether "reasonable doubt" as to the identity of a data subject exists, we request you to also explain this.

3. *We request that you explain in more detail how a data subject can say that they do not wish to provide their ID (even with redactions). On your website it does not look like the data subject has any choice.*
4. *What has happened with the Finnish complainant in this case? Was he removed from the newsletter? Did he receive access to his personal data/have his personal data deleted? If so, how long did it take from when he sent in such requests to when they were resolved?*

On 7 September 2021, NAS responded to our order to provide information dated 20 August 2021 stating that:

- The new solutions relating to the right to be forgotten and the right to access own data will involve including a button on customer accounts to "forget me" and to "access my data". The verification method will be logging on to the customer account. This requires new IT solutions and will involve adjustment in all of NAS' systems that process personal data and external third parties processing personal data on behalf of NAS.
    - For customers without an online account, the identification requirements have not yet been decided upon, but an automated process is the targeted end result meaning that there will not be a requirement to provide ID. The identification of correct data subjects is part of an ongoing DPIA and will be concluded based on the risks identified in the DPIA.
- In relation to the current system of receiving access requests, NAS added that there is a text field where the data subject may object to NAS' requirement to upload a copy of (potentially redacted) ID, and that the request process does not stop if no ID is uploaded.
- In relation to the Finnish complainant, NAS stated that it cannot find any case relating to them in the customer care system which means that they have not submitted a request through NAS' portal. However, the complainant does not receive a newsletter from NAS.

On 27 September 2022, NAS sent us a letter stating that in light of this matter, NAS undertook a further review and assessment of the practice of requiring ID from data subjects in relation to the exercise of data subject rights. Based on such assessment, NAS concluded that they no longer require ID to verify the identity of a data subject in relation to the exercise of data subject rights.

On 14 July 2023, we sent NAS with an advance notice of our intention to adopt a decision to issue a reprimand and invited their comments. NAS responded on 9 August 2023 that they did not have any comments further to their letter of September 2022.

On 11 August 2023, we submitted a draft decision to the other supervisory authorities concerned. The supervisory authority that had originally received the complaint had certain comments to such draft decision, in particular regarding how the issue had been resolved regarding the complainant.

On 30 August 2023, we withdrew the draft decision from IMI due to comments from one supervisory authority. Shortly afterwards, we sent NAS an order to provide information as to how the complainant's original access request had been handled, and whether NAS still processed the complainant's data. If NAS had not handled the complainant's original request, we requested NAS to make contact with the complainant to confirm their details and arrange for a copy of their personal data to be sent to the complainant. In addition, we also asked NAS to confirm with the complainant whether or not they wished to exercise their right to erasure.

On 8 September 2023, NAS responded and stated they could not confirm whether the original request had been complied with and that they could confirm that the complainant still had an active profile with them. NAS further stated that they would contact the complainant again to ensure that complainant's requests are complied with.

The complainant responded to NAS on 4 February 2024 confirming that they wished to exercise their right to access under Article 15 GDPR and then deletion under Article 17 GDPR.

On 12 February 2024, NAS confirmed that the complainant's access and erasure request were complied with on 9 February 2024. At our request, the supervisory authority that received the original complaint contacted the complainant to ask whether they were satisfied with the measures taken by the controller to respect their rights. The complainant did not respond to the complaint receiving supervisory authority within the deadline set.

4. Legal Background

The GDPR has been incorporated into Annex XI to the European Economic Area ("EEA") Agreement by means of Decision of the EEA Joint Committee No 154/2018 ("EEA Joint Committee Decision").[2]

Article 1(b) of the EEA Joint Committee Decision provides that:

> *"[…] the terms "Member State(s)" and "supervisory authorities" shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively."*

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

> *"References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively."*

[2] Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

The Norwegian Personal Data Act (*Nw. personopplysningsloven*) incorporated the GDPR into Norwegian law.[3] The Norwegian Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.[4]

Article 5(1)(c) and (2) GDPR reads as follows:

> 1. *Personal data shall be:*
>
> …
>
> c. *Adequate, relevant and **limited to what is necessary in relation to the purposes** for which they are processed ('data minimisation');*
>
> …
>
> 2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

Article 12(2) and (6) GDPR reads as follows:

> 2. *The controller **shall facilitate the exercise of data subject 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.*
>
> …
>
> 6. *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.*

5. Datatilsynet's Competence

NAS is established in Norway and in the context of its activities it processes personal data. Therefore, the GDPR applies to NAS' data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of the complainant, NAS qualifies as a controller within the meaning of Article 4(7) GDPR, as NAS decided on the means and purposes of the relevant processing of personal data, as acknowledged in NAS' privacy policy at the time of the complaint.[5]

---

[3] Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").
[4] Ibid., § 32.
[5] https://web.archive.org/web/20180425231647/https://www.norwegian.no/booking/bestillingsinformasjon/regler-og-vilkar/personvern/

As a controller, NAS has its main establishment within the meaning of Article 4(16) GDPR in Norway. Moreover, the processing of the personal data of NAS customers, including the complainant, qualifies as cross-border processing under Article 4(23) GDPR. This is because the policies and routines of NAS in relation to the exercise of data subject rights, and more particularly the verification of data subjects, substantially affect or are likely to substantially affect data subjects in more than one EEA state.

Therefore, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to this case and we are competent to act as lead supervisory authority pursuant to Article 56(1) GDPR.

6. The Norwegian Data Protection Authority's assessment

Chapter 3 of the GDPR lays down the rights of data subjects. These rights allow data subjects to retain control over their personal data that is processed by controllers. The right of access under Article 15 GDPR is one of the rights that a data subject can exercise against a controller.

We consider that the complainant's e-mail to NAS dated 25 May 2018 was an access request pursuant to Article 15 GDPR, and that NAS itself interpreted such e-mail as a data subject right request as it responded to the complainant on 11 June 2018 from the e-mail address "data.protection@norwegian.com" requesting additional information from the complainant for the purposes of verifying the identity of the data subject in order for NAS to comply with the request.

Pursuant to Article 12(2) GDPR a controller must facilitate the exercise of the rights of data subjects and shall not refuse to act on the request of a data subject to exercise his or her rights, unless the controller demonstrates that it is not in a position to identify the data subject. In other words, it must be demonstrably impossible for the controller to be able to identify the data subject based on the information already in its possession at the time it receives the data subject request in order to be able to validly refuse to act.

Any verification method must be proportionate to the objective to be achieved, in this case to provide the data subject with access to their personal data pursuant to Article 15 GDPR, and limited to what is necessary in relation to such purpose, i.e. that the purpose cannot reasonably be fulfilled by less harmful or less intrusive means in accordance with Article 5(1)(c) GDPR. Controllers should implement or re-use an authentication procedure in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR insofar as a digital communication channel already exists between the data subject and the controller. In this case, a digital communication channel already existed between the complainant and NAS, in that the complainant's e-mail address was stored in NAS' systems and NAS used the complainant's e-mail address to communicate with the complainant when responding to the complainant's data subject request. Therefore NAS possessed the information it needed to be able to identify the data subject at the time of the Complaint.

If a controller is able to identify the data subject based on the information it already has in its possession, but nevertheless has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject pursuant to Article 12(6) GDPR. It follows that a controller that wishes to rely on Article 12(6) GDPR must therefore conduct a two-stage assessment. Firstly, a controller must determine whether it has reasonable doubts concerning the identity of the natural person making a data subject request. Secondly, if reasonable doubts as to the identity of the person making a data subject request exist, a controller must determine what additional information is *necessary* to be able to confirm the identity of the data subject in accordance with the principle of data minimisation.

NAS did not at the time of the Complaint carry out any individual assessment as to whether it had reasonable doubts regarding the identity of the complainant making a request under Article 15 GDPR. NAS required the complainant to upload an un-redacted copy of their Photo ID before NAS would proceed with responding to the complainant's request. Further, NAS did not inform the complainant that there was any other way of identifying themselves.

We therefore consider that NAS has not demonstrated that it had reasonable doubts as to the complainant's identity in accordance with Article 12(6) GDPR that would have justified it requesting the complainant to provide additional information in order to confirm their identity. Neither do we consider that NAS requesting a copy of the complainant's Photo ID was necessary or proportionate in accordance with Article 5(1)(c) GDPR under the circumstances where there were less intrusive ways of confirming the complainant's identity. NAS could have used other authentication methods to confirm the identity of the data subject without having to resort to requiring the data subject to upload an unredacted copy of their valid Photo ID, such as asking the complainant security questions based on travel history.

In light of the above, we therefore find that NAS:

- Infringed Article 12(6) GDPR by requesting the provision of the complainant's Photo ID without demonstrating that it had reasonable doubts as to the identity of the complainant
- Infringed Article 5(1)(c) GDPR by requesting more information than was necessary in order to confirm the identity of the data subject
- Infringed Article 12(2) GDPR by effectively imposing unnecessarily burdensome measures on the complainant by requiring provision of Photo ID in order to carry out the complainant's request

7. Mitigating factors

NAS has throughout our investigation of the Complaint been cooperative and shown willingness to adjust its routines and policies where necessary.

NAS changed their routines shortly after meeting with us in 2019 to discuss the problems raised by the Complaint, and further changed their routines in 2021 following the comments

of the Danish and Finnish data protection authorities to NAS' practice. In September 2022, NAS informed us that after having undertaken a further review and assessment of the verification of data subjects, NAS no longer requires data subjects to submit a copy of an identification document in relation to the exercise of data subject rights.

8. Corrective Measures

In light of the extent of the infringements identified and taking into account the mitigating factors above, we consider it is appropriate to issue NAS with a reprimand pursuant to Article 58(2)(b) GDPR.

9. Access to Case Documents and Public Access

As a party to the present case, you have the right to access the documents in this case pursuant to Section 18 of the Norwegian Public Administration Act[6].

All documents we possess are subject to freedom of information requests pursuant to Article 3 of the Norwegian Freedom of Information Act.[7] If you believe that this letter or your written representations should be partly or fully exempt from public access, please let us know and explain why you believe such an exemption should be applied.

10. Right of Appeal

As this decision has been adopted by Datatilsynet pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section 22 of the Norwegian Personal Data Act (*Nw. personopplysningsloven*). This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Senior Legal Adviser

This letter has electronic approval and is therefore not signed

Copy to: the complainant

[6] Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).
[7] Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova) § 3.