



Your reference


Our reference
23/00909-11

Date
27.03.2024

Rejection of Complaint - DNB Bank ASA

1. Introduction


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.

 (hereinafter “complainant”) is a customer of DNB Bank ASA (hereinafter “DNB”, “bank” or “controller”) who suspects that one of the bank's employees who carried out consultation operations on her bank account did not actually act under the authority and in accordance with the instructions of DNB. The complainant considers the information provided by the controller to be insufficient to enable her to dispel her doubts as to the lawfulness of the processing of her personal data, and lodged a complaint with Datatilsynet asking that we carry out an investigation to dispel her doubts.

After having requested DNB to provide us with the information we needed in order to examine the complaint, we have found no evidence that one of the bank's employees carried out consultation operations on the complainant's personal data against or beyond the instructions received from DNB.

In light of the above, we have decided that the complaint shall be rejected as unfounded.

2. Decision

Datatilsynet adopts the following decision on the complaint submitted by  against DNB (national case number 23/00909):

- The complaint shall be rejected as unfounded pursuant to Article 60(8) GDPR.

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.

3. Factual Background

In 2019, the complainant asked DNB to provide her with a report on the consultation operations carried out by the employees of the bank on her bank account.

On 25 March 2019, DNB sent the requested report to the complainant. The report indicated the dates and the number of consultation operations carried out on the complainant's bank account.

After having reviewed such a report, the complainant considered that the number of consultation operations was "not normal", and asked DNB to investigate whether there had been any unauthorized access to her personal data.

DNB carried out the requested internal investigation, and on 10 May 2019 it informed the complainant that it did not identify "anything illegal or suspicious" (in Norwegian, "det er ikke avdekket noe ureglementert eller mistenkelig").

The complainant considered the information provided by the controller to be insufficient to enable her to dispel her doubts as to the lawfulness of the processing of her personal data, and lodged a complaint with Datatilsynet asking that we carry out an investigation to dispel her doubts.²

On 26 January 2024, Datatilsynet wrote to the complainant to inform her that, after having reviewed the documentation she produced, Datatilsynet had not identified any elements to call the conclusion reached by DNB's internal investigation into question. Therefore, Datatilsynet intended to close the case.

On 26 January 2024, the complainant wrote to Datatilsynet to express her insistence that Datatilsynet should continue investigating this case. The complainant justified this request on the grounds that she suspected that a female friend of her mother, employed at the "DnB Linderud" office, had been accessing the complainant's bank account many times over the past several years on behalf of the complainant's mother.

On 31 January 2024, Datatilsynet wrote to the complainant to ask her to provide us with the name of the DNB's employee she suspected, and to explain on what grounds she suspected that the employee in question had carried out unauthorized accesses to her bank account. The complainant never responded to this request.

Datatilsynet also wrote to DNB to ask the controller to provide us with a list of employees who had carried out consultation operations on the complainant's bank account since 2019, as well as the dates and purposes of those operations. DNB provided Datatilsynet with such information on 12 February 2024.

² The first communication regarding this case was received by Datatilsynet on 8 March 2023. However, in that communication the complainant referred to a previous letter she sent to Datatilsynet, but which appears to have gone missing.

4. Legal Background

GDPR

Article 5(1)(a) GDPR provides that personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject.

Furthermore, Article 29 GDPR provides as follows:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

The GDPR also establishes the following data subjects' rights, which are relevant in the present case:

Pursuant to Article 12(3) GDPR:

The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Pursuant to Article 15 GDPR:

1. 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, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;*
- (b) the categories of personal data concerned;*
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
- (f) the right to lodge a complaint with a supervisory authority;*
- (g) where the personal data are not collected from the data subject, any available information as to their source;*

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

EEA and Norwegian Law

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”).³

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.

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.⁴ The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet’s Competence

In its letter to DNB of 29 January 2024, Datatilsynet asked DNB to confirm whether the processing at issue in the present case qualifies as “cross-border processing” within the meaning of Article 4(23) GDPR. In its response dated 12 February 2024, DNB confirmed this, and stated that DNB has an office in Latvia whose employees can access the bank’s customer database

³ 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.

⁴ Act No 38 of 15 June 2018 relating to the processing of personal data (“personopplysningsloven”).

and follow the same routines as the bank's employees in Norway. DNB also stated that its main establishment is located in Norway, and that the decisions on the purposes and means of the relevant processing are taken in that establishment, which has the power to have such decisions implemented.

In light of the above, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that DNB's main establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. Therefore, a draft of the present decision was shared with the other supervisory authorities concerned, which did not raise any objections within a period of four weeks after having been consulted in accordance with Article 60(3) GDPR.

6. Datatilsynet's Assessment

At the outset, it must be pointed out that, in accordance with Article 29 GDPR, any person acting under the authority of the controller who has access to personal data may process those data only on instructions from that controller.

Moreover, it should be noted that information on the frequency and intensity of the consultation operations carried out by the employees of the controller may enable the data subject to ensure that the processing carried out is actually motivated by the purposes put forward by the controller.⁵

However, the CJEU has made clear that data subjects do not enjoy an absolute right to obtain from the controller information relating to the identity of the employees who carried out those operations.⁶ This is mainly because:

Even if the disclosure of the information relating to the identity of the controller's employees to the data subject may be necessary for that data subject in order to ensure the lawfulness of the processing of his or her personal data, it is nevertheless liable to infringe the rights and freedoms of those employees.⁷

Nonetheless, the CJEU stated that:

if the data subject were to consider the information provided by the controller to be insufficient to enable him or her to dispel his or her doubts as to the lawfulness of the processing of his or her personal data, he or she has the right to lodge a complaint with the supervisory authority on the basis of Article 77(1) of the GDPR, that authority having the power, under Article 58(1)(a) of that regulation, to request the controller to provide it with any information it needs in order to examine the data subject's complaint.⁸

⁵ CJEU, Case C- 579/21, *Pankki*, para. 70.

⁶ *Ibid.*, para. 83.

⁷ *Ibid.*, para. 79.

⁸ *Ibid.*, para. 82.

It is in light of the above ruling, as well as the doubts expressed by the complainant, that Datatilsynet requested DNB to provide us with the information we needed to examine the complaint.

The information on the consultation operations carried out on the complainant's bank account since 17 May 2018 we obtained from DNB did not reveal any suspicious activity. Essentially all consultation operations were done in response to or in connection with a request from the complainant. No consultation operation had been carried out by someone employed at the "DnB Linderud" office. Moreover, most of the consultation operations had been carried out by male employees or a robot, and no single employee had carried out consultation operations with a very high frequency or intensity.

Therefore, the complainant's suspicions that a female employee of DNB's "DnB Linderud" office had carried out a large number of unauthorized accesses to her bank account appear to be unfounded.

Having considered the above, the complaint shall be rejected as unfounded in accordance with Article 60(8) GDPR.

7. Right of Appeal

As this decision has been adopted pursuant to Chapter VII GDPR, pursuant to Article 22(2) of the Norwegian Data Protection Act, the present decision may not be appealed before the Privacy Appeals Board (in Norwegian: *Personvernemda*). However, the present decision may be challenged before Oslo District Court (in Norwegian: *Oslo tingrett*) in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act and Article 4-4(4) of the Norwegian Dispute Act (in Norwegian: *tvisteloven*).⁹

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

This letter has electronic approval and is therefore not signed

Copy to: DNB BANK ASA

⁹ See Section 22 of the Act of 15 June 2018 No. 38 relating to the processing of personal data (in Norwegian: *personopplysningsloven*).