Datatilsynet

SATS ASA
Postboks 4949 NYDALEN

0423 OSLO

Your reference	Our reference	Date
	20/02422-9	06.02.2023

Administrative Fine - SATS 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.

Between 2 October 2018 and 8 December 2021, Datatilsynet received several complaints against SATS ASA (hereinafter "SATS", "you", "your", "the company"). In essence, all such complaints concerned alleged infringements of data subjects' rights committed by SATS, in particular in connection with its handling of data subjects' requests submitted pursuant to Articles 15 and 17 GDPR.

After having investigated all of these complaints, Datatilsynet hereby issues an administrative fine of NOK 10 000 000 (ten million) against SATS for having violated Articles 5(1)(a) and (e), 6(1), 12, 13, 15 and 17 GDPR.

2. Datatilsynet's Decision

Pursuant to Article 58(2)(i) GDPR, Datatilsynet issues an administrative fine of NOK 10 000 000 (ten million) against SATS ASA for:

- having infringed Articles 12(3) and 15 GDPR by failing to timely act upon two separate access requests;

- having infringed Articles 5(1)(e), 12(3) and 17 GDPR by failing to take prompt action and erase certain personal data without undue delay pursuant to three separate erasure requests;

[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.

- having infringed Articles 5(1)(a), 12(1) and 13 GDPR by failing to duly inform data subjects about its data retention policy concerning the personal data of banned members, and the relevant legal basis for the processing; and

- having infringed Articles 5(1)(a) and 6(1) GDPR by failing to rely on a valid lawful basis to process the training history data of the members of its fitness centers.

Our inquiry has only focused on SATS' compliance with Articles 5, 6, 12, 13, 15 and 17 GDPR in connection with the complaints against SATS lodged with Datatilsynet between 2 October 2018 and 8 December 2021. Thus, the present decision is without prejudice to the possibility of opening future inquiries into SATS' compliance with other provisions of the GDPR and with respect to other data subjects.

3. Factual Background

On 2 October 2018, Datatilsynet received a complaint against SATS (Case 20/01746, previously 18/03153).[2] This complaint was submitted by a member of the fitness centers run by SATS in Norway (hereinafter "Complainant No 1") who essentially claimed that in May 2018 (or earlier), SATS Norway AS (i.e., an entity of SATS' corporate group)[3] had transferred their personal data to other companies within its corporate group, as well as to Facebook outside the EU/EEA, without a proper legal ground.[4] Complainant No 1 also claimed that an access request they submitted on 29 August 2018 to privacy@satselixia.no pursuant to Article 15 GDPR has remained unanswered.[5]

On 1 March 2019, Datatilsynet received another complaint against SATS (Case 20/02422, previously 19/00817).[6] This complaint was submitted by another member of the fitness centers run by SATS in Norway (hereinafter "Complainant No 2") who essentially claimed that SATS failed to respond to an access request they submitted on 25 February 2019 pursuant to Article 15 GDPR, and refused to comply with an erasure request they submitted on the same date pursuant to Article 17 GDPR, after they had their membership terminated by SATS.[7]

On 7 October 2019, Datatilsynet received yet another complaint against SATS (Case 20/01707, previously 19/03020).[8] This complaint was submitted by another member of the fitness centers run by SATS in Norway (hereinafter "Complainant No 3") who essentially claimed that SATS refused to comply with an erasure request they submitted to SATS on 5 October 2019 pursuant to Article 17 GDPR, after they had their membership terminated by SATS.[9]

[2] See letter to Datatilsynet dated 2 October 2018 (hereinafter "Complaint No 1").
[3] When the complaint was lodged with Datatilsynet SATS Norway AS was named HFN Norway AS.
[4] See Complaint No 1.
[5] Ibid.
[6] See email to Datatilsynet dated 1 March 2019 (hereinafter "Complaint No 2").
[7] Ibid.
[8] See email to Datatilsynet dated 7 October 2019 (hereinafter "Complaint No 3").
[9] Ibid.

On 7 September 2021 and 5 October 2021, Datatilsynet formally approached SATS and asked the company to express its views on the issues raised in Complaint No 2 and Complaint No 3.[10] We received SATS' replies on 1 December 2021.[11]

On 8 December 2021, Datatilsynet received one more complaint against SATS (Case 21/04061).[12] This complaint was submitted by yet another member of the fitness centers run by SATS in Norway (hereinafter "Complainant No 4") who essentially claimed that SATS refused to comply with an erasure request they submitted on 6 August 2021 pursuant to Article 17 GDPR.

On 23 March 2022, Datatilsynet sent further questions to SATS on all of the above complaints.[13] We received SATS' response on 28 April 2022.[14]

Given that all of the above complaints concerned partially similar alleged infringements of data subjects' rights committed by SATS, Datatilsynet decided to handle all of these complaints jointly, also for reasons of procedural efficiency. Moreover, as the GDPR and its novel international data transfer requirements became applicable in Norway on 20 July 2018, Datatilsynet decided not to investigate the part of Complaint No 1 dealing with an alleged unlawful transfer of personal data that took place in May 2018 (or earlier).[15] However, this is without prejudice to the possibility of opening future inquiries into SATS' compliance with data transfer requirements.

After having investigated all of these complaints, on 26 September 2022, Datatilsynet sent SATS an advance notification of its intention to issue an administrative fine of NOK 10 000 000 (ten million) against SATS for having violated several provisions of the GDPR.[16]

On 31 October 2022, SATS submitted written representations to Datatilsynet regarding the contested violations and envisaged administrative fine. The present decision takes account of such written representations.[17] However, in our view, SATS' submissions do not warrant any significant changes in our assessment of the present case, as outlined in further detail below.

On 30 December 2022, Datatilsynet submitted a draft decision—which was in line with the above advance notification—to the other supervisory authorities concerned in accordance with Article 60(3) GDPR. None of the other supervisory authorities concerned expressed a relevant and reasoned objection to the draft decision within four weeks after having been consulted by Datatilsynet. Thus, Datatilsynet is bound by that draft decision,[18] which is mirrored in the present decision.

---

[10] See Datatilsynet's letters to SATS dated 7 September and 5 October 2021.
[11] See SATS' letters to Datatilsynet dated 1 December 2021.
[12] See email to Datatilsynet dated 8 December 2021 (hereinafter "Complaint No 4").
[13] See Datatilsynet's letter to SATS dated 23 March 2022.
[14] See SATS' letter to Datatilsynet dated 28 April 2022.
[15] See also Article 57(1)(f) GDPR, which specifies that supervisory authorities should investigate complaints "to the extent appropriate".
[16] See Datatilsynet's letter to SATS dated 26 September 2022.
[17] See SATS' letter to Datatilsynet dated 31 October 2022.
[18] See Art. 60(6) GDPR.

4. Legal Background

4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

> "[…] *applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*."

Moreover, Article 3(1) GDPR provides that the Regulation:

> "[…] *applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*."

4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

> "'*personal data' means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

Pursuant to Article 4(2) GDPR:

> "*'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*"

Pursuant to Article 4(7) GDPR:

> "*'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

Pursuant to Article 4(11) GDPR:

> "*'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*."

Pursuant to Article 4(16) GDPR:

> *"'main establishment' means:*
>
> *(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;* […]".

Pursuant to Article 4(23) GDPR:

> "*'cross-border processing' means either:*
>
> *(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
>
> *(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*"

4.3. Lawfulness of Processing, Information Obligations and Data Subjects' Rights

Article 5(1) GDPR reads as follows:

> "*1. Personal data shall be:*
>
> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Moreover, Article 6(1) GDPR reads:

"*1. Processing shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.* […]"

Further, Article 12(1) and (3) GDPR reads:

> "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*
>
> […]
>
> *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*."

Article 13(1)(c) and (2)(a) GDPR provides:

> "*1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
>
> […]
>
> *(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
>
> […]
>
> 2. *In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:*
>
> *(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period* […]."

Furthermore, Article 15 GDPR reads:

"*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."

In addition, Article 17 GDPR reads:

"*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 following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims."

4.4. Competence, Tasks and Powers of Supervisory Authorities under the GDPR

Pursuant to Article 55(1) GDPR:

> "*Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*."

Further, Article 56(1) GDPR reads as follows:

> "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*."

Pursuant to Article 58(2) GDPR:

> "*2. Each supervisory authority shall have all of the following corrective powers:*
>
> *(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*
>
> *(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;*
>
> *(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;*
>
> *(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;*
>
> *(e) to order the controller to communicate a personal data breach to the data subject;*
>
> *(f) to impose a temporary or definitive limitation including a ban on processing;*
>
> *(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;*
>
> *(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;*

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation."

Pursuant to Article 83(1) to (5) GDPR:

"1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). […]"

4.5. 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").[19]

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.[20] The Personal Data Act and the GDPR became applicable in Norway on 20 July 2018.[21]

5. Datatilsynet's Competence

SATS runs a chain of fitness centers. It has its headquarter in Norway, but has also operations and offices in Denmark, Finland and Sweden.[22]

Thus, SATS has several establishments in the EU/EEA, including in Norway, and in the context of the activities of these establishments it processes personal data, including the personal data of its customers (i.e., the about 700 000 members of its fitness centers), such as the complainants. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of the complainants, SATS (i.e., the controlling undertaking of the SATS group) qualifies as a controller (within the meaning of Article 4(7) GDPR), as it is SATS that had a factual influence on and decided the means and

[19] 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.
[20] Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").
[21] Ibid., § 32.
[22] See SATS' letter to Datatilsynet dated 28 April 2022.

purposes of the relevant personal data processing, as acknowledged in SATS' privacy policy.[23] The company has not disputed SATS' controller status in the context of Datatilsynet's inquiry.[24]

As a controller, SATS has it main establishment (within the meaning of Article 4(16) GDPR) in Norway.[25] Moreover, the processing of the personal data of SATS members, including the complainants, qualifies as cross-border processing under Article 4(23) GDPR. This is because, although all complainants are members of SATS' fitness centers in Norway, SATS members' personal data may be accessed by SATS' staff in all of the European countries in which SATS operates, and SATS' internal routines and policies on data storage, erasure and access are the same in all of the European countries in which SATS operates.[26]

Therefore, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case, and Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. This was not disputed by SATS in the course of our inquiry.[27]

6. Datatilsynet's Assessment

6.1. Findings of a Violation of Articles 12(3) and 15 GDPR

The evidence collected by Datatilsynet shows that Complainant No 1 and Complainant No 2 each submitted an access request to SATS, on 29 August 2018 and 25 February 2019.[28] Both requests were explicit in demanding either information on the recipients of the complainant's personal data and the legal ground for sharing their personal data with such recipients,[29] or a copy of the personal data of the complainant.[30] In this regard, it should be noted that, in order to make an access request under the GDPR, it is sufficient for the requesting data subjects to specify that they want to obtain information on the processing of their personal data, and it is

[23] See SATS' privacy policy from September 2021 (attached to Complaint No 4), which states (in Norwegian): "Denne personvernerklæringen er ment å gi informasjon om hvordan og hvorfor SATS Group AS («SATS Group») samler inn og behandler personopplysninger. Det er SATS Group v/CEO som er behandlingsansvarlig for opplysninger som samles inn og behandles av SATS Group." Note that, on 11 October 2022, SATS' Nordic Head of Legal & Compliance informed us that SATS Group AS does not exist any longer, and that all correspondence should instead be addressed to SATS ASA.

[24] Cf. SATS' letters to Datatilsynet dated 1 December 2021, 23 March 2022, 28 April 2022 and 31 October 2022.

[25] See SATS' letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): "SATS har sin hovedadministrasjon i Oslo og den aktuelle behandlingen blir utført fra samme sted, slik at «hovedvirksomheten» er i Norge i personvernforordningens forstand").

[26] See SATS' letter to Datatilsynet dated 28 April 2022.

[27] Cf. SATS' letter to Datatilsynet dated 31 October 2022.

[28] See correspondence attached to Complaint No 1 and Complaint No 2.

[29] See Complainant No 1's email to privacy@satselixia no dated 29 August 2018 (stating: "I would like to receive information on the parties that my personal data has been shared with, categories of data sent to those parties, as well as legal grounds for such sharing").

[30] See Complainant No 2's email to SATS' Customer Service Manager (i.e., the SATS' employee who notified them of the revocation of their SATS membership) dated 25 February 2019 (stating: "Personopplysninger skal være forsvarlig innhentet og korrekt, men her bygger Sats utestengelsen alene på betjeningen sin versjon av saken uten kontradiksjon. Dette er i strid med personopplysningsloven. Jeg ber derfor om innsyn og kopi av samtlige opplysninger i sakens anledning med; innhold, dato og klokkeslett").

not necessary to specify the legal basis of the request.[31] Further, both requests were submitted through communication channels made available by SATS for similar inquiries.[32] In this respect, it should be pointed out that if a data subject makes a request using a communication channel provided by the controller, such request should be considered effective and the controller should handle such a request accordingly.[33] Therefore, the access requests at hand were effective and validly submitted for the purpose of Article 15 GDPR.

When Datatilsynet asked SATS whether it responded to such access requests, SATS replied that it was unable to confirm that it had taken action with respect to the access request submitted by Complainant No 1.[34] SATS further confirmed this in the written representations it sent to Datatilsynet on 31 October 2022.[35] This is despite the fact that Complainant No 1 sent several reminders to SATS.[36] In essence, according to the evidence collected by Datatilsynet, that access request has remained unanswered to this date.

In its written representations, SATS argued that it is arbitrary from the part of Datatilsynet to contest a violation of Articles 12(3) and 15 GDPR due to a failure to respond to an access request that was submitted around a month after the GDPR became applicable in Norway, as at that time many companies experienced challenges in applying the new rules.[37] We take note of this argument, but find it untenable. As acknowledged by SATS itself, the fact that other companies faced challenges with adapting to the GDPR after it became applicable in 2018 is not a valid justification for a violation of the GDPR that started to occur in September 2018.[38] Moreover, it should be stressed that SATS has never replied to the access request of Complainant No 1—not even after Datatilsynet contacted SATS in connection with Compliant No 1—with the result that that violation is still ongoing, and therefore it does not only concern SATS' failure to act in 2018. Further, it should be noted that Norwegian data subjects enjoyed a right of access also under the Norwegian Data Protection Act from 2000, which was in force before the GDPR became applicable in Norway. [39] Thus, this was not a completely new right that SATS had to become familiar with only after the GDPR became applicable; the company should have had appropriate routines in place to timely respond to access requests since 2001.[40] In passing, it should be emphasized that Datatilsynet's enforcement action in the present case

[31] EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, para. 50.
[32] That is the email privacy@satselixia no, and the email address of SATS' Customer Service Manager who notified to Complainant No 2 the termination of their membership.
[33] EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, paras. 52-57.
[34] See SATS' letter to Datatilsynet dated 28 April 2022.
[35] See SATS' letter to Datatilsynet dated 31 October 2022 (stating (in Norwegian): "SATS erkjenner at man ikke kan dokumentere svaret på innsynsforespørselen fra klager 1").
[36] See correspondence attached to Complaint No 1.
[37] See SATS' letter to Datatilsynet dated 31 October 2022.
[38] Ibid. (stating (in Norwegian): "Det bør bemerkes at forespørselen kom én måned etter GDPR trådte i kraft. SATS var på den tiden ikke alene med å ha utfordringer med å implementere og operasjonalisere sine nye personvernrutiner. SATS forstår at det i utgangspunktet ikke er unnskyldende, men […]" (emphasis added)).
[39] Cf. Sections 16 and 18 of the Norwegian Data Protection Act (LOV-2000-04-14-31) (repealed).
[40] Cf. Section 50 of the Norwegian Data Protection Act (LOV-2000-04-14-31) (repealed). In should be noted that Complainant No 1 submitted an access request also under the rules in force before July 2018. See the correspondence attached to Complaint No 1.

was triggered by complaints submitted by data subjects—which Datatilsynet is required to investigate to the extent appropriate and with all due diligence[41]—and it is not the result of an "arbitrary" *ex officio* initiative aimed at singling out SATS' state of compliance.

As for the second access request, SATS first responded that it did not receive any access request from Complainant No 2,[42] and later noted that it responded to the access request of Complainant No 2 on 27 February 2019.[43] Further, in its written representations, SATS acknowledged that it did not respond satisfactorily to the access request from Complainant No 2.[44] However, the company noted that the request from Complainant No 2 was handled, half a year after the GDPR became applicable in Norway, by SATS' customer service, which at that time was probably less aware of GDPR requirements than others within the organization; something that—according to SATS—was common to most Norwegian companies at the time.[45] We take note of this argument, but find it unconvincing. At the outset, it should be noted that there were approximately two years between the entry into force of the GDPR in 2016[46] and the moment in which it started to apply in 2018.[47] Therefore, companies had at least two years to adapt to the new rules, and European supervisory authorities have repeatedly stated that there would be no "grace period" after the GDPR became applicable in 2018.[48] Moreover, as previously noted, the alleged similar challenges experienced by other businesses with the implementation of the GDPR are no valid excuse for a violation committed by SATS. Moreover, as part of its accountability duties,[49] it was SATS' responsibility to ensure that its personnel in charge of handling customers' inquiries was sufficiently aware of and trained to comply with data subjects' rights, also in view of the fact that—as noted above—the right of access was not a completely new right introduced by the GDPR.

At any rate, in Datatilsynet's view, SATS did not take adequate action in response to the access request from Complainant No 2 without undue delay. Most notably, it did not provide any information on action taken on the request to receive a copy of their personal data that Complainant No 2 submitted to SATS.[50] The email that SATS sent to Complainant No 2 on 27 February 2019 was mainly a response to the complainant's erasure request (see section 6.2 below), and did not provide all of the information that the data subject requested and was

[41] See Article 57(1)(f) GDPR. See too CJEU, Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, para. 109.
[42] See SATS' letter to Datatilsynet dated 1 December 2021 (stating (in Norwegian): "SATS har ikke registrert å ha mottatt en anmodning om innsyn").
[43] See SATS' letter to Datatilsynet dated 28 April 2022.
[44] See SATS' letter to Datatilsynet dated 31 October 2022 (stating (in Norwegian): "SATS erkjenner også at man ikke svarte fullgodt på innsynsforespørselen fra klager 2").
[45] Ibid.
[46] See Art. 99(1) GDPR.
[47] See Art. 99(2) GDPR and § 32 personopplysningsloven.
[48] See e.g.: <https://www.theparliamentmagazine.eu/news/article/gdpr-no-period-of-grace-following-entry-into-force>; <https://www.natlawreview.com/article/happy-gdpr-day>.
[49] See Arts. 5(2) and 24 GDPR.
[50] In this regard, it should be noted that the EDPB has opined that "The controller shall react and, as a general rule, provide the information under Art. 15 without undue delay, which in other words means that the information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so." See EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, para. 156.

entitled to receive under Article 15 GDPR.[51] That email simply provided a brief description of the incident that led to the termination of the SATS membership of Complainant No 2, and a small extract of some parts of SATS' general terms and conditions, as well as information on SATS' internal data retention policy regarding the personal data of banned members. In this regard, it should be noted that "the controller should always be able to demonstrate, that the way to handle the request aims to give the broadest effect to the right of access and that it is in line with its obligation to facilitate the exercise of data subjects rights"[52] and that "the notion of a copy has to be interpreted in a broad sense".[53] In its written representations, SATS took issue with the fact that, in its advance notification of an administrative fine, Datatilsynet referred to the latter two passages in the EDPB's Guidelines 01/2022 on the right of access, which—according to SATS—do not reflect the wording of the GDPR, although SATS did not explain why.[54] In this respect, Datatilsynet notes that, although they are not binding, EDPB guidelines are important interpretative aids[55] that supervisory authorities should take into account to make sure that they comply with their legal obligation to ensure the consistent application of the GDPR throughout the EU/EEA.[56] Further, in our view, the statements made in such passages directly follow from the obligation to facilitate the exercise of data subjects rights set out in Article 12(2) GDPR, as well as from the broad effect that should be given to the data subject's right of access so as to ensure that such a right "retains its effectiveness" and to "enable the data subject to check […] that the data concerning him or her are accurate", which implies that the "the information provided must be as precise as possible".[57] This is also because Article 15 "gives specific expression" to the individual right to access data concerning him or her, enshrined in the second sentence of Article 8(2) of the Charter of Fundamental Rights of the European Union,[58] as well as Article 8 ECHR.[59] In any event, it should be stressed that SATS did not provide any copy whatsoever—narrow or broad—of the personal data it processed, as expressly requested by Complainant No 2 and required by Article 15(3) GDPR.

[51] Cf. SATS' Customer Service Manager's email to Complainant No 2 dated 27 February 2019 (attached to Complaint No 2).
[52] EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, para. 35.
[53] Ibid., para. 25.
[54] See SATS' letter to Datatilsynet dated 31 October 2022.
[55] EDPB guidelines are even used as interpretative aids by European high courts. See e.g. CJEU, Case C-645/19, *Facebook Ireland and Others*, para. 74; CJEU, Case C-911/19, ECtHR, *Biancardi v. Italy, Application no. 77419/16*, judgment of 25 November 2021, paras. 29 and 53.
[56] See Arts. 51(2) and 70(1)(d)-(m). See too, by analogy, CJEU, Case C-911/19, *Fédération bancaire française (FBF) v Autorité de contrôle prudentiel et de résolution (ACPR)*, para. 71.
[57] Opinion of Advocate General Pitruzzella in Case C-154/21, *RW v Österreichische Post AG*, paras. 19 and 26.
[58] Ibid., para. 14.
[59] ECtHR*, K.H. and Others v. Slovakia*, App. No. 32881/04, para. 47.

Finally, it should be pointed out that SATS acknowledged that its handling of both of the above access requests was not entirely satisfactory,[60] and that such requests could have been better handled.[61]

In light of the above, SATS violated Articles 12(3) and 15 GDPR with respect to Complainant No 1 and Complainant No 2, as it failed to take adequate action on the access requests they submitted on 29 August 2018 and 25 February 2019 within the deadline set out in Article 12(3).

In its written submissions, SATS argued that Datatilsynet's conclusion that SATS violated both Article 12(3) and 15 GDPR would violate the principle of *ne bis in idem* (in Norwegian "dobbeltstraff").[62] This argument should be rejected. At the outset, it should be recalled that "the principle *ne bis in idem* […] do[es] not apply to a situation in which several penalties are imposed in a single decision, even if those penalties are imposed for the same actions. In fact, where the same conduct infringes several provisions punishable by fines, the question whether several fines may be imposed in a single decision falls not within the scope of the principle *ne bis in idem*".[63] Indeed, neither that principle nor the principle governing concurrent offences "preclude an undertaking from being penalised for an infringement of several distinct legal provisions, even if those provisions have been infringed by virtue of the same conduct."[64] This is even specifically envisaged in Article 83(3) GDPR, which provides that "[i]f a controller […] for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement" (emphasis added). In any event, Articles 12(3) and 15 GDPR must necessarily be read (and applied) together—and may thus be cumulatively violated—as the first provision regulates the timing for taking action on an access request, whereas the second provision establishes what kind of information must be provided in response to such a request.

6.2. Findings of a Violation of Articles 5(1)(e), 12(3) and 17 GDPR

The evidence collected by Datatilsynet shows that Complainant No 2, Complainant No 3 and Complainant No 4 each submitted a data erasure request to SATS, on 25 February 2019, 5 October 2019 and 6 August 2021. In its written representations, SATS wrongly claimed that the erasure requests were "only two",[65] whereas the erasure requests assessed by Datatilsynet were three.[66]

---

[60] See SATS' letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): "SATS [er] åpen for at det kan ha skjedd mindre glipper i håndteringen av anmodninger fra de fire klagerne saken gjelder, i relasjon til respons tid og begrunnelser").
[61] See SATS' letter to Datatilsynet dated 31 October 2022 (stating (in Norwegian): "SATS erkjenner at medlemmenes forespørsler kunne vært bedre håndtert").
[62] Ibid., p. 9.
[63] GC, Case T-704/14, *Marine Harvest ASA v European Commission*, para. 344. See too CJEU, Case C-10/18 P, *Mowi ASA v European Commission*.
[64] GC, Case T-704/14, *Marine Harvest ASA v European Commission*, paras. 370-371. See too GC, Case T-609/19, *Canon v European Commission*, para. 461; CJEU, Case C-10/18 P, *Mowi ASA v European Commission*.
[65] See SATS' letter to Datatilsynet dated 31 October 2022, p. 3 (stating (in Norwegian): "her er det snakk om kun *to* forhold").
[66] See Complaints No 2, No 3 and No 4.

The erasure requests of Complainant No 2 and Complainant No 3 concerned all of their personal data, and were submitted after the termination of their SATS membership by SATS. Conversely, the erasure request of Complainant No 4 was not submitted in connection with any termination of their membership, and concerned only specific kinds of personal data, namely the logs of their training activities.

SATS eventually responded to all of such requests,[67] although SATS replied for the first time to Complainant No 4 – after a reminder from the complainant[68] – on 23 September 2021,[69] i.e. more than one month after it received their request on 6 August 2021, which constitutes in itself a violation of Article 12(3) GDPR.[70]

In its reply to Complainant No 3 dated 11 October 2019, SATS refused to delete the complainant's date of birth, name and picture, and justified this on the basis of the following internal policy, which was copied verbatim (in English) in the text of the email to the complainant:

> "If the customer relationship is terminated due to improper behavior from the member, name, date of birth and picture shall be kept for 60 months. Further, the member in question shall be marked as 'excluded'. The rest of the data shall be deleted, included possible reports on the behavior."[71]

Complainant No 3 was further informed by SATS that, based on the above internal policy, SATS could retain their date of birth, name and picture for 60 months, whereas the rest of their personal data would be deleted within 30 days.[72] SATS also informed the same complainant that they would be banned from SATS' fitness centers for 24 months from the date in which they received SATS' notification of the termination of their membership.[73]

Complainant No 2 received a partially similar response. Most notably, in its reply to Complainant No 2 dated 27 February 2019, SATS stated that:

---

[67] SATS replied to the erasure requests of Complainants No 2 and No 3 within the deadline set out in Article 12(3) GDPR, but failed to take adequate action upon such requests, as outlined below.
[68] See Complainant No 4's email to SATS dated 16 September 2021 (attached to Complaint No 4).
[69] As acknowledged by SATS. See SATS's letter to Datatilsynet dated 28 April 2022.
[70] Article 12(3) GDPR provides that "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" (emphasis added). Datatilsynet has taken into account the relatively modest duration of SATS' delay when setting the amount of the administrative fine issued against SATS (see Section 7.1 below).
[71] See email from kundeservice@sats no to Complainant No 3 dated 11 October 2019 (attached to SATS' letter to Datatilsynet dated 1 December 2021).
[72] Ibid.
[73] Ibid. (stating (in Norwegian): "du vil være utestengt fra SATS i 24 måneder fra datoen vi sendte deg informasjon om utestengelsen per brev").

> "Banned members can, in accordance with the GDPR, request to have their training history deleted, while other information and the member profile itself can be retained by us for up to 60 months".[74]

SATS also informed Complainant No 2 that they would be banned from SATS' fitness centers for one year starting from 21 February 2019.[75]

When asked by Datatilsynet to explain the purposes for which SATS retained and processed the personal data of banned members (including Complainant No 2 and Complainant No 3), SATS stated:

> "SATS processes the date of birth, name and photo [of the former member] in connection with [their] exclusion, with the aim of being able to prevent the excluded member from using SATS' services during the exclusion period" (emphasis added).[76]

After having been notified of our intention to issue an administrative fine, SATS (knowingly)[77] changed position, and stated that a broader and vaguer purpose applies in this context: "the purpose of the storage is to be able to process the information in connection with the ban. This purpose does not expire as soon as the ban is lifted".[78] It also claimed that such a change of position would not affect the assessment of the legitimacy of the retention period.[79] We disagree with the latter claim: any broadening of the scope of the purpose of a processing operation inevitably affects such an assessment. This is because personal data must be kept for "no longer than is necessary for the purposes for which the personal data are processed"[80] (emphasis added), with the result that the necessity of the retention must be assessed vis-à-vis the relevant purpose. Furthermore, it is not possible to adjust the relevant purpose *ex post*; the assessment should be made with respect to the purpose identified by the controller at the outset of the relevant processing, as it results from the evidence collected by the supervisory authority during its investigation. Moreover, the answer that SATS provided to Datatilsynet in April 2022 specifically addressed the purpose of processing the personal data of Complainant No 2 and Complainant No 3—which SATS identified as "being able to prevent the excluded member from using SATS' services during the exclusion period"—whereas in its written representations from October 2022 SATS described the purpose of processing the personal data of banned members in general. In this respect, Datatilsynet acknowledges that, in certain exceptional

---

[74] SATS' email to Complainant No 2 dated 27 February 2019 (our translation) (stating (in Norwegian): "Utestengte medlemmer kan i henhold til GDPR be om å få sin treningshistorikk slettet, mens annen informasjon og selve medlemsprofilen kan beholdes av oss i inntil 60 måneder").

[75] SATS' email to Complainant No 2 dated 21 February 2019 (stating (in Norwegian): "Du er utestengt for 1 år fra dagens dato").

[76] See SATS' letter to Datatilsynet dated 28 April 2022 (our translation) (stating (in Norwegian): "SATS behandler fødselsdato, navn og bilde i forbindelse med utestengelse, for det formål å kunne forhindre det utestengte medlemmet fra å benytte seg av SATS' tjenester i løpet av utestengelsesperioden").

[77] See SATS' letter to Datatilsynet date 31 October 2022, p. 3 (stating (in Norwegian): "SATS beklager at formålet er noe snevrere angitt i SATS' svar av 28. april 2022 til Datatilsynet").

[78] Ibid. (stating (in Norwegian): "[…] er formålet med oppbevaringen å kunne behandle opplysningene i forbindelse med utestengelsen. Dette formålet utløper ikke straks utestengelsen er opphevet").

[79] Ibid. (stating (in Norwegian): "dette har naturligvis ingenting å si for den rettslige vurderingen av om oppbevaringstiden er legitim").

[80] See Art. 5(1)(e) GDPR.

circumstances, SATS may need to process the personal data of banned members for purposes that go beyond preventing them from using SATS' services during the exclusion period (e.g. to defend a legal claim in court, etc.). However, this would not apply invariably in all cases, and most importantly it does not apply in this case, given that, when asked about the purpose for which SATS processed the data of Complainant No 2 and Complainant No 3, SATS replied that it processed such data to be "able to prevent the excluded member from using SATS' services during the exclusion period". Therefore, in the present case, Datatilsynet will exclusively focus on the latter purpose.

A company running a fitness center may legitimately retain and refuse to delete the date of birth, name and photo of former members who were banned from its fitness center for the entire duration of the relevant ban. This is because such information is essential to enable the center's staff to enforce the ban. However, retaining such personal data for a period longer than the duration of the ban, or retaining more than the aforementioned personal data (e.g., training logs, correspondence, etc.), violates the storage limitation principle set out in Article 5(1)(e) GDPR (unless the data are retained for other legitimate purposes beyond preventing the excluded member from using the center's services during the exclusion period). This is because the personal data at hand would no longer be necessary for the purposes for which they are/were processed.

Whether SATS legitimately refused to act – at least partially – upon the erasure requests submitted by Complainant No 2 and Complainant No 3 should also be assessed in light of the actual necessity of processing their data, as the GDPR's right of erasure applies *inter alia* where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.[81]

In the present case, in our view, SATS failed to comply with Articles 17 and 5(1)(e) GDPR with respect to the personal data of both Complainant No 2 and Complainant No 3.

Despite the fact that Complainant No 3 required the erasure of all of their personal data on 5 October 2019, and that SATS informed them on 11 October 2019 that their personal data other than their date of birth, name and picture would be deleted within 30 days, SATS deleted Complainant No 3's training logs, membership number, address, telephone number and e-mail only on 4 November 2021,[82] after the opening of Datatilsynet's inquiry. In this regard, it should be noted that "SATS acknowledges that certain member data on complainant […] No 3 were stored beyond SATS' internal routines".[83] Thus, with respect to the erasure of such data, SATS did not take action without undue delay, as required by Article 17(1) GDPR.

Moreover, SATS retained the date of birth, name and picture of Complainant No 3 beyond the relevant exclusion period of 24 months—as such data were deleted on 4 November 2021 (i.e., after Datatilsynet's inquiry) and the exclusion period started running on 4 October 2019—even though such data were processed "with the aim of being able to prevent the excluded member

[81] See Art. 17(1)(a) GDPR.
[82] See SATS' letter to Datatilsynet dated 28 April 2022.
[83] See SATS' letter to Datatilsynet dated 31 October 2022, p. 3 (stating (in Norwegian): "erkjenner SATS at visse medlemsdata om klager […] 3 ble lagret utover SATS' internrutiner.").

from using SATS' services during the exclusion period", with the result that such data were retained for longer than it was necessary for the purpose for which the data were processed, in breach of Article 5(1)(e) GDPR.

Similarly, despite the fact that Complainant No 2 required the erasure of all of their personal data on 25 February 2019, and that the above-cited SATS' internal policy provides that personal data other than the date of birth, name and picture "shall be deleted" after the member's exclusion, SATS retained the "address and telephone number"[84] of Complainant No 2 until 4 November 2021.[85] It also retained the correspondence with Complainant No 2, at least until 2021.[86] In this respect, it should be noted that "SATS acknowledges that certain member data on complainant No 2 […] were stored beyond SATS' internal routines".[87] SATS claimed that this was likely due to a mistake, which was presumably due to the extraordinary workload during the Covid-19 pandemic.[88] However, Datatilsynet finds that the pandemic is an irrelevant factor in this respect, given that the personal data at hand should have been deleted without undue delay from 25 February 2019, i.e. long before the beginning of the pandemic in Norway. Moreover, SATS retained the date of birth, name and picture of Complainant No 2 well beyond the relevant exclusion period of one year, as such data were deleted on 4 November 2021 (i.e., after Datatilsynet's inquiry) and the exclusion period started running on 21 February 2019. Thus, such data were retained for longer than it was necessary for the purpose for which the data were processed, in breach of Article 5(1)(e) GDPR, given that they were processed "with the aim of being able to prevent the excluded member from using SATS' services during the exclusion period".[89]

In its written representations, SATS argued that the assessment of the necessity of a storage period is to a large extent discretionary, and that Datatilsynet is not in the position to and should refrain from questioning the assessment made by the controller.[90] In this respect, it should be noted that, while it is for the controller to ensure operational compliance with its data retention obligations, the controller must also be able to *demonstrate* compliance with such obligations to the supervisory authority,[91] and thus allow the authority to review whether the retention periods set by the controller are justified. Consequently, Datatilsynet is competent to review the assessment made by the controller to ensure compliance with its retention obligations. In the present case, Datatilsynet has simply reviewed the necessity of the retention of the data of Complainants No 2 and 3 in light of: (1) the relevant purpose of the processing identified by SATS, which is linked to a specific timeframe ("being able to prevent the excluded member from using SATS' services during the exclusion period" (emphasis added)); and (2) SATS'

[84] See SATS' letter to Datatilsynet dated 1 December 2021 (stating (in Norwegian): "Klager ble utestengt fra SATS' sentre den 20. februar 2019 grunnet truende oppførsel motto av SATS' ansatte. Utestengelsen ble registrert i SATS' medlemssystem Exerp. Ved utestengelse lagrer SATS navn, fødselsdato, adresse og telefonnummert").
[85] Ibid.
[86] Excerpts from such correspondence were included by SATS in its reply to Datatilsynet dated 1 December 2021.
[87] See SATS' letter to Datatilsynet dated 31 October 2022, p. 3 (stating (in Norwegian): "erkjenner SATS at visse medlemsdata om klager 2 […] ble lagret utover SATS' internrutiner.").
[88] See SATS' letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): "ser det ut til a ha skjedd en glipp som antagelig skyldes den ekstraordinære arbeidsmengden under pandemien").
[89] See SATS' letter to Datatilsynet dated 28 April 2022 (our translation).
[90] See SATS' letter to Datatilsynet dated 31 October 2022, p. 4.
[91] See Art. 5(2) GDPR.

retention policy, which provided that personal data other than the date of birth, name and picture "shall be deleted" after the member's exclusion. Moreover, SATS itself has acknowledged that it has retained some of the personal data of Complainants No 2 and 3 for longer than its own internal routines envisaged. Therefore, Datatilsynet has not determined the necessity of the relevant retention periods in the abstract, in light of its own subjective evaluations; it has merely tested the necessity of the relevant retention periods in light of the information and justifications provided by the controller.

In our view, SATS also violated Articles 17 and 5(1)(e) GDPR with respect to Complainant No 4. This is for the reasons outlined below.

As explained in more detail below (see section 6.4), SATS' general terms and conditions allow its members to withdraw consent to the processing of their training history data and request that such data be deleted. Thus, in our view, Complainant No 4 legitimately relied on this provision to withdraw their consent and request the deletion of their training history data on 6 August 2021:

> "Jeg […] trekker herved tilbake mitt samtykke til at SATS kan behandle, lagre eller på annen måte oppbevare følgende personopplysninger:
>
> - Sporing av hvilket treningssenter jeg trener på
> - Sporing av hvilke tidspunkter jeg trener på
> - Annen overvåkning av min treningsaktivitet […]
>
> Vennligst bekreft at dette er mottatt, at ovennevnte personopplysninger vil bli slettet fra og med uke 31, og at ovennevnte personopplysninger ikke vil bli innhentet, lagret, oppbevart eller på andremåter behandlet fra og med uke 31".[92]

In light of such request, SATS should have deleted the complainant's training history data without undue delay in accordance with Article 17(1)(b) GDPR. Instead, SATS replied to Complainant No 4 that the deletion would take place within 6 months in accordance with its privacy policy, and explained that such a deletion deadline was set among other things for ensuring the safety of SATS members and infection tracing during the pandemic.[93] SATS also informed Complainant No 4 that Article 17(1)(b) was not applicable to their case, as SATS' legal basis for processing their training history data was "Article 6(1)(b) and (f)", and the processing was still necessary in relation to the purposes for which they were collected or otherwise processed.[94]

---

[92] See Complainant No 4's email to privacy@sats no dated 6 August 2021 (attached to Complaint No 4).

[93] See SATS' email to Complainant No 4 dated 23 September 2021 (stating (in Norwegian): "Sletting skjer i henhold til vårpersonvernerklæring senest etter 6 måneder ved mottatt anmodning om sletting […] Bakgrunnen for […] slettefristen på 6 måneder etter mottatt krav om sletting, er blant annet sikkerheten til våre medlemmer samt smittesporing ").

[94] See SATS' email to Complainant No 4 dated 2 October 2021 (stating (in Norwegian): "Vi har tidligere forklart deg grunnlaget for oppbevaringen i inntil seks måneder fra vi har mottatt en sletteanmodning, som – blant andre forhold – er knyttet til sikkerheten til våre medlemmer samt smittesporing. Dette er hensyn som faller innenfor artikkel 17 nr. 1 a) i personvernforordningen (GDPR), som «nødvendige for formålet de ble samlet inn eller behandlet for», sammenholdt med behandlingsgrunnlaget i artikkel 6 nr. 1 bokstav b) og f). Som konsekvens av

In our view, SATS' position on the applicability of Article 6(1)(b), and accordingly on the inapplicability of Article 17(1)(b), is untenable in this case (see further section 6.4 below). Moreover, while the retention for a few months of the training logs of the previous last few weeks or months for infection tracing purposes may be justified in the context of the Covid-19 pandemic, the blanket retention for up to 6 months (after an erasure request) of all available training logs appears unjustified and disproportionate.[95] Indeed, data retention for infection tracing purposes should be proportionate to the incubation and infectious period of Covid-19, which was deemed to require a quarantine period of 14 days for those who had a close contact with an infected individual in the last 24 hours.[96] The excessiveness of a retention period of 6 months is further supported, for example, by the fact that the Regulation on Digital Infection Tracing provided for a data retention period of up to 30 days.[97] While SATS insisted in its written representations that 6 months was a necessary and proportionate retention period, it did not provide any evidence or specific arguments to support its view.[98] In any event, it should be noted that SATS deleted the training history data of Complainant No 4 only on 7 April 2022, i.e. after the opening of our inquiry and well beyond the 6 months deadline specified by the company.[99] However, SATS stated that this was due to a mistake.[100]

In conclusion, based on the evidence collected by Datatilsynet, it appears that SATS did not properly handle any of the above three erasure requests. In this regard, it should be noted that SATS itself has acknowledged that its handling of these erasure requests was not entirely satisfactory.[101] While, if taken in isolation, each of these episodes of mishandling of a data subject's request is not very grave, the fact that they have occurred repeatedly over a long period of time and have affected multiple data subjects is indicative of broader, more systemic issues regarding SATS' handling of data subjects' requests. Moreover, it bears emphasizing that SATS proceeded to delete the personal data of all of the above complainants with a considerable delay, only after Datatilsynet's inquiry. It would have likely retained such data for even longer without our intervention.

---

at det på denne bakgrunn foreligger et lovlig formål for behandlingen og utsatt sletting, har du heller ikke et krav på omgående sletting i medhold av artikkel 17 nr. 1bokstav b).").

[95] Note that Complainant No 4 has been a member of SATS for about 8 years. Thus, they likely generated a considerable amount of training logs over these years, and SATS' retention of the training logs for infection tracing purposes was not limited to the previous last few weeks or months.

[96] Forskrift om smitteverntiltak mv. ved koronautbruddet (Covid-19-forskriften). In our guidelines on infection tracing published on 21 September 2020 we wrote that "It will not normally be necessary to store information about visitors for infection control reasons for more than 14 days". See Datatilsynet, Besøksregistrering og smittesporing (21.09.2020) (stating (in Norwegian): "Det vil normalt ikke være nødvendig å lagre opplysninger om besøkende av smittevernhensyn i mer enn 14 dager") <https://www.datatilsynet no/personvern-pa-ulike-omrader/korona/besoksregistrering-og-smittesporing/>.

[97] Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19.

[98] SATS simply stated (in Norwegian) "SATS' vurdering om lagringstid er uansett rimelig og forsvarlig, og da er det ikke avgjørende om Datatilsynet skulle ha et noe avvikende syn på tidens lengde". Cf. SATS' letter to Datatilsynet dated 31 October 2022, p. 4.

[99] See SATS' letter to Datatilsynet dated 28 April 2022.

[100] Ibid.

[101] See SATS' letter to Datatilsynet dated 28 April 2022 (stating: "SATS [er] åpen for at det kan ha skjedd mindre glipper i håndteringen av anmodninger fra de fire klagerne saken gjelder, i relasjon til respons tid og begrunnelser").

In its written submissions, SATS argued that Datatilsynet's conclusion that SATS breached Articles 5(1)(e), 12(3) and 17 GDPR would violate the principle of *ne bis in idem*.[102] This argument should be rejected. As noted above, that principle does not preclude an undertaking from being penalised for an infringement of several distinct legal provisions, even if those provisions have been infringed by virtue of the same conduct.[103] Moreover, it should be noted that Article 12(3) and 17 GDPR must necessarily be read (and applied) together—and may thus be cumulatively violated—as the first provision regulates the timing for providing information on the action taken on a request under Article 17, whereas the second provision establishes upon what conditions the right to erasure set out in Article 17 applies.

As for the contested violation of Article 5(1)(e), SATS also argued that "it will always be the case that a breach of a specific obligation [in the GDPR] also represents a breach of one of the privacy principles" and therefore the two breaches should not be cumulated.[104] This argument should be rejected. If one would follow SATS' argument, a violation of Article 5 should never be contested. However, this would deprive Article 83(5)(a) of essentially any effect, as the latter provision establishes a specific fine for infringements of "the basic principles for processing […] pursuant to Article 5".[105] It must be clear that, in our view, the basic principles in Article 5 are both general rules that shall guide the reading of other provisions in the GDPR *and* legal requirements in their own right. In particular, Article 17 should be read jointly and in light of the principle set out in Article 5(1)(e), but the latter provision may also be breached on its own. This has occurred in the present case with respect to the personal data that SATS could legitimately retain for a while after the relevant erasure request (e.g., date of birth, name and photo of banned members), but that it eventually retained for much longer than it was actually necessary. Finally, it should be noted that the EDPB has already found that the same conduct may lead to the simultaneous breach of a principle in Article 5 and of the obligations stemming from that principle in the rest of the GDPR.[106]

6.3. Findings of a Violation of Articles 5(1)(a), 12(1), 13(1)(c) and 13(2)(a) GDPR

It is apparent from the evidence collected by Datatilsynet that SATS has established a specific data retention policy with respect to the personal data of members whose membership is terminated by SATS. The policy reads as follows:

> "If the customer relationship is terminated due to improper behavior from the member, name, date of birth and picture shall be kept for 60 months. Further, the member in

[102] See SATS' letter to Datatilsynet dated 31 October 2022, p. 9.
[103] GC, Case T-704/14, *Marine Harvest ASA v European Commission*, paras. 370-371. See too GC, Case T-609/19, *Canon v European Commission*, para. 461.
[104] See SATS' letter to Datatilsynet dated 31 October 2022, p. 9 (stating in Norwegian: "Det vil så å si alltid være slik at et brudd på en konkret forpliktelse også representerer brudd på et av personvernprinsippene. Datatilsynet må naturligvis påse at man ikke anser ett og samme forhold som to brudd på GDPR og regner dette dobbelt i sin vurdering av overtredelsesgebyr.").
[105] See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, para. 191.
[106] See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, paras. 183-201.

question shall be marked as 'excluded'. The rest of the data shall be deleted, included possible reports on the behaviour".[107]

This policy was apparently developed by SATS in cooperation with an external law firm[108] and appears to be a standard internal policy given that all of SATS' replies to the erasure requests mentioned above refer to this 60 months retention period, and that the policy at hand was quoted in English in an email in Norwegian to a Norwegian data subject,[109] which—in our view—may indicate that SATS' customer service copied it from an internal document in English.

Nonetheless, no publicly available documents (including SATS' privacy policy and terms of service) provide specific information on the retention period at hand, as acknowledged by SATS.[110] In this respect, SATS initially noted that the duration of the exclusion of a member may vary and that therefore it is impossible to provide general information on the storage period applicable to the personal data of banned members, and that in any event SATS' privacy policy mentions that personal data are stored for as long as it is necessary for achieving the purposes for which they are obtained.[111] However, in its written representations, SATS acknowledged that it should have been more transparent on this point.[112]

For the sake of clarity and completeness, Datatilsynet notes that SATS was not sufficiently transparent regarding its data retention policy for the following reasons. First, given that SATS formalized such a retention policy internally, one may not logically argue that it is impossible to inform data subjects of such policy in advance, as this could have been done for example by simply copying the above-quoted wording in SATS' privacy policy. Secondly, to comply with Article 13(2)(a) GDPR, it is not sufficient to state that personal data will be stored for as long as necessary, without providing any additional information that would enable the data subject to assess, on the basis of their own situation, the retention period for specific data or purposes.[113]

Therefore, in our view, SATS violated Articles 5(1)(a) and 13(2)(a) GDPR, as it failed to ensure transparency about the period for which it stores the personal data of banned members and/or the criteria used to determine that period. Under Article 13(1) GDPR, such information should have been provided "at the time when personal data are obtained". Therefore, it is not sufficient to inform data subjects about this retention period when SATS notifies them of the termination of their membership.

On a general note, Datatilsynet has strong reservations about a blanket storage period of 60 months for personal data of banned members. This is because 60 months is an extraordinarily

[107] See email from kundeservice@sats.no to Complainant No 3 dated 11 October 2019 (attached to SATS' letter to Datatilsynet dated 1 December 2021).
[108] Ibid. See too SATS' letter to Datatilsynet dated 31 October 2022, p. 5.
[109] See email from kundeservice@sats no to Complainant No 3 dated 11 October 2019 (attached to SATS' letter to Datatilsynet dated 1 December 2021).
[110] See SATS' letter to Datatilsynet dated 28 April 2022.
[111] Ibid.
[112] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating in (Norwegian) "På dette punktet tar SATS selvkritikk. […] Det er på det rene at slettetidene skulle vært mer konkrete").
[113] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, As last Revised and Adopted on 11 April 2018), p. 38.

long period, which in practice may lead SATS to retain such data for longer than it is necessary, in violation of Article 5(1)(e), as exemplified by how SATS handled the erasure of the data of Complainant No 2 and Complainant No 3 (see section 6.2 above). A retention period of 60 months would only be justifiable in very exceptional circumstances, whereas much shorter retention periods should apply in standard cases. Thus, specific criteria should be set out, and communicated in advance to data subjects, to ensure that the data of banned members are not processed for longer than it is actually necessary in practice, in light of the circumstances of the specific termination of the membership. However, it is for the controller to identify and apply the relevant criteria.

Moreover, SATS' privacy policy in effect in 2021 simply stated that SATS' legal basis for processing the personal data of its customers was generally "performance of a contract" and in some cases "consent" (see further section 6.4 below).[114] However, the policy did not clarify which processing activities or purposes were covered by each of these legal bases. This constitutes in itself a breach of Articles 12(1) and 13(1)(c) GDPR, as the information on legal bases in the privacy policy was not "clear" and did not allow data subjects to assess, on the basis of their own situation, what legal basis/purposes apply.[115] This confusion was further exacerbated by the fact that, when questioned about the applicable legal basis by a data subject, SATS also referred to a legal basis (i.e., legitimate interest) that was not mentioned among the relevant legal bases listed in its privacy policy.[116] Nonetheless, SATS' current privacy policy (updated after the opening of our inquiry) is clearer on this point.[117] In its written representations, SATS acknowledged that "the description [in its privacy policy in effect in 2021] of the legal grounds should have been more refined".[118] However, it claimed that the recent update to its privacy policy was not triggered by Datatilsynet's inquiry.[119]

In its written representations, SATS argued that Datatilsynet's conclusion that SATS breached Articles 5(1)(a), 12(1), 13(1)(c) and 13(2)(a) GDPR would violate the principle of *ne bis in idem*.[120] Moreover, SATS argued that "all violations of Article 13 automatically constitute a breach of Article 12" and that "it will always be the case that a breach of a specific obligation

[114] See Personvernerklæring og informasjonskapsler – SATS (attached to Complaint No 4).
[115] Cf. Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, As last Revised and Adopted on 11 April 2018), page 9.
[116] See correspondence attached to Complaint No 4.
[117] See: <https://www.sats no/legal/personvernerklaring> (stating: "Vi må ha behandlingsgrunnlag etter GDPR for vår behandling av personopplysninger. For *administrasjon av medlemskap, treningsoppfølgning, online trening, app-funksjoner* og *treningsrelaterte tjenester* er grunnlaget at det er nødvendig for å oppfylle vår avtale med deg. For *kjøp* er det nødvendigheten av å oppfylle en rettslig forpliktelse. For *produktutvikling* er det vår berettigede interesse i forbedring og innovasjon. For *studier* er det vår berettigede interesse å bidra til forskning og folkeopplysning. For *kameraovervåkning* er det behovet for å forebygge farlige situasjoner og å ivareta hensynet til våre ansatte og medlemmers sikkerhet. Om det er nødvendig for oss å behandle særlige kategorier av personopplysninger (sensitive personopplysninger) for å yte våre tjenester til deg, er behandlingsgrunnlaget ditt samtykke som du gir via medlemsvilkårene (GDPR artikkel 6 nr. 1 bokstav a og artikkel 7 nr. 4).").
[118] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating in (Norwegian) "På dette punktet tar SATS selvkritikk. […] beskrivelsen av behandlingsgrunnlagene skulle vært mer raffinert").
[119] Ibid.
[120] See SATS' letter to Datatilsynet dated 31 October 2022, p. 9.

[in the GDPR] also represents a breach of one of the privacy principles".[121] Therefore, according to SATS, these breaches should not be cumulated. These arguments should be rejected. As noted above, the principle of *ne bis in idem* does not preclude an undertaking from being penalised for an infringement of several distinct legal provisions, even if those provisions have been infringed by virtue of the same conduct.[122] Moreover, it should be noted that Articles 12(1) and 13 must be read (and applied) together—and may thus be cumulatively violated—as the first provision regulates *how* certain information must be provided, whereas the second provision establishes *what* information must be provided.

As for the violation of the transparency principle in Article 5(1)(a), we emphasize once again that there is nothing in the GDPR that precludes a controller from being penalized both for an infringement of a principle in Article 5 and an infringement of the obligations stemming from that principle in the rest of the GDPR.[123] In the present case, by failing to provide sufficient information about the relevant storage periods and legal basis for the processing, SATS has not only violated the specific information requirements laid down in Article 13(1)(c) and (2)(a) GDPR; it also failed to ensure that "personal data [are] processed […] in a transparent manner in relation to the data subject", as required pursuant to Article 5(1)(a) GDPR.

6.4. Findings of a Violation of Articles 5(1)(a) and 6(1) GDPR

Complainant No 4 lodged their complaint with Datatilsynet, partly due to their doubts regarding SATS' position on the legal basis for the processing and storage of training history data.[124] We believe that Complainant No 4 has raised legitimate doubts regarding SATS' position on such legal basis. This is due to the fact that SATS' privacy policy and general terms and conditions provide confusing and misleading information on this point. Furthermore, SATS has provided partially different responses regarding the legal basis for the processing of training history data to Complainant No 4 and to Datatilsynet. This warrants an assessment of whether SATS relied on a valid legal basis for processing training history data.

SATS' privacy policy in effect in 2021 stated the following with respect to the legal bases that SATS relied on for processing the personal data of its customers:

> "**RETTSLIG GRUNNLAG FOR BEHANDLING AV PERSONOPPLYSNINGER**
>
> Behandling av personopplysninger er ikke tiltatt med mindre det foreligger et gyldigbehandlingsgrunnlag. Et slikt behandlingsgrunnlag kan eksempelvis være samtykke fra den registrerte, kontrakt (inngåelse av avtale), lov eller at vi som

[121] Ibid. (stating (in Norwegian): "Det vil så å si alltid være slik at et brudd på en konkret forpliktelse også representerer brudd på et av personvernprinsippene […] alle brudd på artikkel 13 automatisk utgjør brudd på artikkel 12").
[122] GC, Case T-704/14, *Marine Harvest ASA v European Commission*, paras. 370-371. See too GC, Case T-609/19, *Canon v European Commission*, para. 461.
[123] See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, paras. 183-201.
[124] See correspondence attached to Complaint No 4.

> behandlingsansvarlig har en «berettiget interesse» som overstiger den registrertes krav på personvern.
>
> Vårt behandlingsgrunnlag er i hovedsak kontrakt, og i noen tilfeller samtykke. Ved oppstart av behandling av dine personopplysninger vil vi alltid gi informasjon om behandlingsgrunnlag."[125]

Therefore, the privacy policy simply stated that SATS' legal basis for processing the personal data of its customers was generally "performance of a contract" and in some cases "consent", but without specifying which purposes were covered by each of these legal bases.

However, Section 5.2 of SATS' general terms and conditions in effect in 2021 stated:

> "Medlemmet samtykker til at SATS, og andre firmaer som inngår i samme konsern, registrerer, lagrer og bruker opplysninger om Medlemmet […] Medlemmet samtykker til at SATS lagrer treningshistorikk med det formål å kunne følge opp Medlemmets aktivitet og tilrettelegge Medlemmets treningsopplegg")[126] (In the English version: "The Member consents to that SATS and other companies that are part of the same Group, registering, storing and using such personal data […] The Member agrees that SATS can save training history data in order to be able to monitor Member activities and facilitate Member training").[127]

Moreover, Section 5.3 of SATS' general terms and conditions read:

> "Medlemmet har rett til innsyn i sin treningshistorikk og kan kreve å få denne slettet. SATS skal bekrefte mottak av melding om sletting."[128] (In the English version: "The Member can withdraw consent to their training history and request that such be deleted. SATS will confirm receipt of notification in respect of deletion").[129]

This wording ("samtykker"/"consent") in the general terms and conditions suggests that the processing of training history data to monitor member activities and facilitate member training is one of those processing activities for which SATS relied on "consent" as a legal basis.

However, during our inquiry, SATS took the view that the term "samtykker"/"consent" in the general terms and conditions should not be interpreted as "consent" for GDPR purposes, and that SATS' legal basis for processing training history data was Article 6(1)(b) GDPR.[130] Nonetheless, in its written representations, SATS acknowledged that its communication regarding legal bases was imprecise.[131]

---

[125] See Personvernerklæring og informasjonskapsler – SATS (attached to Complaint No 4).
[126] Generelle vilkår for medlemskap i SATS – SATS (attached to Complaint No 4).
[127] SATS's General Terms and Conditions (English Version), applicable from 23.08.2021, available at <https://www.sats.no/legal/english-version-of-our-general-terms-and-conditions>.
[128] Generelle vilkår for medlemskap i SATS – SATS (attached to Complaint No 4).
[129] SATS's General Terms and Conditions (English Version), applicable from 23.08.2021, available at <https://www.sats.no/legal/english-version-of-our-general-terms-and-conditions>.
[130] See SATS' letter to Datatilsynet dated 28 April 2022.
[131] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5.

In addition, in its written representations, SATS claimed that it is up to the controller to determine the relevant legal basis, and that Datatilsynet is not in the position to challenge the controller's choice regarding the legal basis, as long as the latter is reasonable and justified.[132]

Datatilsynet takes note of these arguments, but find them unconvincing. Although it is the controller's responsibility to ensure that it relies on a valid legal basis,[133] the validity of the legal basis chosen by the controller (and hence the lawfulness of the processing) may be verified and challenged by supervisory authorities,[134] as well as by data subjects.[135] Thus, it is not the case that Datatilsynet is not in the position to challenge the validity of the legal basis chosen by SATS. Moreover, the legal basis must be identified and communicated to data subjects at the outset of the processing;[136] it is not possible for the controller to "fix" the legal basis *ex post*. Therefore, the supervisory authority's assessment of the lawfulness of the processing should inevitably focus on the choice made by the controller at the outset of the processing, which should be assessed *inter alia* on the basis of the information that the controller has provided to data subjects.

With respect to the processing of training history data, SATS' general terms and conditions in effect in 2021 provides that SATS members "samtykker"/"consent" to the processing of such data. That wording is included in a section of the general terms and conditions with the heading "personopplysning, markedsføring og kommunikasjon", which exclusively deals with data protection and privacy matters. Thus, it seems illogical that the terms used in that section should not be interpreted in accordance with their standard meaning under data protection law, as SATS argued. Moreover, the English version of that section expressly states that consent can be withdrawn,[137] which further confirms that the section uses the term "consent" in accordance with the GDPR.[138] Finally, the fact that consent to the processing of training history data can be withdrawn under SATS' general terms and conditions confirms that such processing is not necessary for the performance of the membership contract, as outlined further below.

It should be noted that for consent to be valid under the GDPR it should generally be separate.[139] In this regard, the EDPB has opined that "the situation of 'bundling' consent with acceptance

---

[132] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating in Norwegian: "GDPR legger opp til at det er den behandlingsansvarlige som fastsetter sine behandlingsgrunnlag. Tilsynet kan neppe overprøve slike vurderinger så lenge de er forsvarlige og rimelige").

[133] See Arts. 5(1)(a) and (2), 6 and 24 GDPR.

[134] See Art. 57(1)(a) GDPR. See too e.g. CJEU, Case C-245/20, *X, Z v Autoriteit Persoonsgegevens*, para. 22 (assuming that supervisory authorities are generally competent to "review the lawfulness" of a processing operation, barring when the latter is carried out by a court in its judicial capacity).

[135] See Recital 63 GDPR (stating: "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing" (emphasis added)).

[136] See EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para. 17.

[137] SATS's General Terms and Conditions (English Version), applicable from 23.08.2021, Section 5.3 (stating: "The Member can withdraw consent to their training history and request that such be deleted").

[138] See Article 7(3) GDPR.

[139] See Article 7(4) and Recital 43 GDPR. See further Case C-673/17, *Planet49* (Advocate General Opinion), para. 66.

of terms or conditions, or 'tying' the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given".[140]

Therefore, the consent to the processing of training history data set out in Section 5.2 and tied to the acceptance of SATS' general terms and conditions is invalid, as – contrary to what SATS argued[141] – such processing is not invariably and objectively necessary to perform the contract.[142] This is first and foremost evidenced by the fact that, as outlined above, SATS' general terms and conditions allow members to withdraw their consent to the processing of the training history data and request that such data be deleted. In this regard, it should be noted that the general terms and conditions do not specify that any conditions apply to requests for deletion, they simply provide that SATS shall acknowledge receipt of such requests. Moreover, SATS' processing of training history data is not objectively necessary to provide its services, at least to those members who intend to make only a basic use of SATS' training facilities (e.g., without participating in group classes, without using a personal trainer, etc.), as access to SATS' facilities to simply work out on one's own does not require the recording of training history data. Furthermore, in its written representations, SATS stated that the processing of such data is "relevant"[143] to offer its services, but it failed to explain or show how such processing would be "necessary" to perform the contract with its members.[144] In this respect, the EDPB has opined that:

> "necessary for the performance of a contract with the data subject […] must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance. […] Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract."[145]

---

[140] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Adopted on 4 May 2020, para. 26.

[141] See SATS' letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): "lagring om treningshistorikk er nødvendig for at SATS skal kunne tilby en integrert del av sin tjeneste, nemlig treningsoppfølging. SATS tilbyr segregerte medlemskap, f.eks. medlemskap forbeholdt ett senter, sentre i en region eller medlemskap på landsbasis. I tillegg tilbyr SATS en rekke tilleggstjenester, f.eks. gruppetimer, PT-timer et c. SATS må følgelig behandle opplysninger om treningshistorikk (dvs. besøk og økter) for a blant annet holde oversikt over at medlemmets tilgang kjøpte og gjennomført e gruppetimer, PT-timer etc.").

[142] See EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para. 27 (stating: "Where a controller seeks to establish that the processing is based on the performance of a contract with the data subject, it is important to assess what is objectively necessary to perform the contract").

[143] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating (in Norwegian): "SATS mener at behandling av treningshistorikk er relevant for å tilby medlemmene treningsoppfølging, som er en sentral del av SATS' tjenester» (emphasis added).

[144] It should be emphasised that the controller is responsible to demonstrate compliance with the lawfulness principle. See Article 5(2) GDPR.

[145] See EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para. 28.

In its written representations, SATS claimed that the EDPB's strict interpretation of Article 6(1)(b) has no basis in the GDPR.[146] Datatilsynet takes note of this argument. However, it should be dismissed in light of the case law of the CJEU on the notion of 'necessity of processing personal data'. Indeed, the CJEU has repeatedly found that "[a]s regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary" (emphasis added).[147]

In light of the above, neither Article 6(1)(a) nor Article 6(1)(b) was a valid legal basis for SATS' processing of training history data in the circumstances at hand, as the consent to such processing was not "freely given" and "informed", as it was tied to the general acceptance of SATS' terms and conditions, and in any event the processing at hand was not objectively necessary to the performance of the membership contract. Therefore, SATS violated Articles 5(1)(a) (lawfulness principle) and 6(1) GDPR, as it failed to have a valid legal basis in place to engage in the processing of training history data.

The fact that SATS failed to have a valid legal basis in place is further evidenced by the fact that, in response to a query from Complainant No 4, SATS noted that the legal bases for processing and retaining training history data was "Article 6(1)(b) and (f)",[148] and the latter (i.e., Art. 6(1)(f)) was neither mentioned as a relevant legal basis in the privacy policy nor in the general terms and conditions. This shows that the applicable legal basis was unclear also to SATS' staff.

It should be pointed out in passing that the choice of an appropriate legal basis is not a mere "technicality" of very limited importance to data subjects, as suggested by SATS.[149] Rather, it is essential to ensure compliance with a core principle of the GDPR (i.e., the lawfulness principle), which is of key importance to data subjects, as evidenced by the fact that Complainant No 4 took issue with the legal bases that SATS communicated to them. In any event, it is for SATS to identify an appropriate legal basis, should it wish to process training history data in the future.[150]

---

[146] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5.

[147] CJEU, Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, para. 30 (and case law cited therein).

[148] See SATS' email to Complainant No 4 dated 10 October 2021 (referring to "behandlingsgrunnlaget i artikkel 6 nr. 1 bokstav b) og f)") (attached to Complaint No 4).

[149] See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating (in Norwegian): "Under enhver omstendighet kan det ikke være tvilsomt at GDPR artikkel 6(1)(f), berettiget interesse, er et gyldig behandlingsgrunnlag for treningshistorikk. Uenighet om gråsonene mellom artikkel 6(1)(b) og 6(1(f) er langt på vei en "teknikalitet" med svært begrenset betydning, om noen, for medlemmene.").

[150] In its written representations, SATS sought Datatilsynet's input on whether Article 6(1)(f) could be an appropriate legal basis to process training history data in the future. See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating (in Norwegian): "SATS er åpen for heller å basere behandlingen av treningshistorikk på artikkel 6(1)(f) dersom Datatilsynet skulle mene at dette grunnlaget er mer treffende").

In its written submissions, SATS argued that Datatilsynet's conclusion that SATS breached Articles 5(1)(a) and 6(1) GDPR would violate the principle of *ne bis in idem*.[151] Moreover, SATS argued that "it will always be the case that a breach of a specific obligation [in the GDPR] also represents a breach of one of the privacy principles" [152] and therefore the two breaches should not be cumulated.[153] In this respect, it is sufficient to restate what has been mentioned above with respect to the other violations of Article 5: there is nothing in the GDPR that precludes a controller from being penalized both for an infringement of a principle in Article 5 and an infringement of the obligations stemming from that principle in the rest of the Regulation.[154] In the present case, by failing to have a valid legal basis for the processing of training history data, SATS has not only failed to make sure that "personal data [are] processed lawfully", as required by Article 5(1)(a); it also failed to make sure that one of the legal bases listed in Article 6(1) could validly be invoked.

7. Choice of Corrective Measure

Under Article 58(2) GDPR, Datatilsynet has several corrective powers, including the power to impose administrative fines for violations of the GDPR.

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, due regard must be given to the factors listed in Article 83(2)(a) to (k) GDPR. The following sub-sections outline how Datatilsynet has given "due regard" to these factors in the present case.

7.1. Nature, Duration and Gravity of the Infringements (Art. 83(2)(a))

As regards the criterion at Article 83(2)(a), SATS' infringements consist in having failed to comply with requirements whose violations may all be sanctioned in accordance with the higher tier of sanctions (Article 83(5)) under the GDPR's two-tier sanctions' system. In this regard, it should be noted that the GDPR "in setting up two different maximum amounts of administrative fine (10/20 million Euros), already indicates that a breach of some provisions of the Regulation may be more serious than for other provisions".[155] This only speaks to the intrinsic nature of some infringements (i.e., the infringements that may be fined up to 20 million Euros are— according to the assessment made by the legislator— by "nature" more serious than those that may be fined up to 10 million Euros). However, the actual gravity of a specific infringement should be assessed having regard also to other elements;[156] whether a violation is subject to a

[151] See SATS' letter to Datatilsynet dated 31 October 2022, p. 9.
[152] Ibid. (stating (in Norwegian): "Det vil så å si alltid være slik at et brudd på en konkret forpliktelse også representerer brudd på et av personvernprinsippene").
[153] Ibid.
[154] See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, paras. 183-201.
[155] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 9.
[156] It should be noted that "nature" and "gravity" are two different and separate elements in Article 83(2)(a) GDPR.

maximum fine of 20 or 10 million Euros is only a starting point for assessing its gravity.[157] With respect to the nature of SATS' infringements, it should also be noted that the infringements at hand concern "rights and obligations [that] are at the core of the fundamental right to data protection".[158] We consider that, overall, SATS' infringements may be deemed to be moderately serious in nature in the present circumstances.

The duration of most of the infringements is considerable. The access request of Complainant No 1 has remained unanswered since 2018, and SATS never provided a copy of the personal data of Complainant No 2 in response to their request in February 2019, although these data were finally deleted on 4 November 2021. SATS replied to Complainant No 4 only a couple of weeks late. However, SATS deleted certain personal data of Complainant No 2 and of Complainant No 3 on 4 November 2021, respectively about one and nineteen months after the expiry of the relevant exclusion period when the deletion should have taken place. As for the infringements of the lawfulness and transparency requirements, these are partially ongoing and have lasted at least since August 2021 (i.e., since the last update to the general terms and conditions). Such a – on the whole – prolonged state of noncompliance is one of the key elements to be taken into consideration in the analysis of the gravity of the infringements.

The gravity of the infringements should be assessed bearing in mind that they relate to rights and obligations that are at the core of the fundamental right to data protection. However, the impact of the infringements for the affected individuals, or at least for the complainants, appears to have been relatively modest in practice, as Datatilsynet has not been made aware of any specific damages suffered by the data subjects, apart from the emotional distress incurred, although the excessive retention of data on alleged wrongdoing could have had significant consequences for the relevant data subjects (e.g., a prolonged exclusion from the fitness centers). While the former element attenuates to a certain extent the gravity of the infringements, a central element of the analysis of their gravity should be whether the nature and scope of the infringements are indicative of broader, more systemic issues. In this regard, Datatilsynet considers that a multinational company, like SATS, should have sufficient policies, procedures and routines in place to enable the company to promptly and adequately respond to data subjects' requests, and to meet the relevant storage limitation, transparency and lawfulness requirements.

In its written representations, SATS claimed that the identified infringements are not indicative of more systemic issues, as the present case concerns only a very small number of complaints.[159] However, in our view, the reoccurrence over a long period of time of several similar failures to ensure compliance with key data protection rights and obligations reveals that the infringements were not the result of occasional oversights. Instead, they are indicative of a failure to put in

[157] This is noted in response to SATS' remark that the seriousness of a violation may not be assessed only on the basis of whether it may be sanctioned under Article 83(4) or (5). Cf. SATS' letter to Datatilsynet dated 31 October 2022.

[158] EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, Adopted on 13 October 2021, para. 2 (stating: "Data protection cannot be ensured without adhering to the rights and principles set out in the GDPR (Articles 12 to 22 […], as well as Article 5 in so far as its provisions correspond to the rights and obligations provided in Articles 12 to 22 GDPR). All these rights and obligations are at the core of the fundamental right to data protection").

[159] See SATS' letter to Datatilsynet dated 31 October 2022, p. 6.

place and follow adequate policies, procedures and routines. Moreover, through the assessment of the four complaints at issue in the present case, Datatilsynet has identified compliance issues that go beyond the mishandling of a few data subjects' requests (e.g., a failure to have a valid lawful basis in place for the processing of training history data in general, deficiencies in policies and documents that apply or applied to all of SATS' members, etc.). This is a systemic issue that enhances the gravity of the infringements. In this regard, it should be noted that most of the complaints concern data subjects' requests and policies that predate the Covid-19 pandemic. Thus, the pandemic should not be factored in when assessing the gravity of the infringements.

In respect of the number of affected data subjects, most of the violations affected four individuals in Norway (i.e., the complainants). However, some violations (i.e., the infringement of the transparency and lawfulness obligations) have affected virtually all of the about 700 000 SATS members.

Having considered the above, and taking into account all of the aforementioned aggravating and mitigating elements in their complexity, Datatilsynet considers the infringements to be moderately grave. This factor should be weighed accordingly in the present case.

7.2. Intentional or Negligent Character of the Infringements (Art. 83(2)(b))

In respect of the criterion at Article 83(2)(b), the EDPB found that:

> "*In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*"[160]

Further to our inquiry, we see no evidence of an intentional infringement on the part of SATS. However, in our view, the infringements arose due to negligence on the part of SATS, insofar as the company failed to implement and follow appropriate measures to respond timely and properly to data subjects' requests, and to ensure – and be able to demonstrate – full compliance with storage limitation, lawfulness and transparency requirements, thus disregarding its duty of care.[161] However, further to our inquiry, SATS seems to have taken some measures to improve its routines and state of compliance (see section 7.3 below).

It bears emphasizing that several staff members of SATS, including SATS' Customer Service Manager, have been involved in handling the above data subjects' requests, and that SATS' management is ultimately responsible for ensuring SATS' compliance with the GDPR. SATS has itself stated that the CEO has a responsibility for GDPR compliance.[162] Therefore, it may

[160] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 12. These guidelines have been endorsed by the EDPB. See EDPB, Endorsement 1/2018 (adopted on 25 May 2018).
[161] See Article 5(4) and 24 GDPR.
[162] Generelle vilkår for medlemskap i SATS – SATS (attached to Complaint No 4) (stating: "Databehandlingsansvarlig for opplysningene er SATS v/CEO.").

be concluded that several staff members of SATS have acted negligently in connection with the establishment and implementation of adequate compliance measures, as they disregarded their duty of care to ensure compliance with several legal obligations under the GDPR.[163]

Overall, this factor should be weighed moderately against SATS in the present case.

In its written representations, SATS claimed that the negligence identified by Datatilsynet should be weighed neither against nor in favor of SATS. Datatilsynet disagrees with this view, and considers that the identified negligence should be weighed against SATS, albeit moderately. This is because SATS acted negligently over a prolonged period of time, despite the fact that several data subjects prompted SATS to bring its processing into compliance. Thus, the infringements are not due to a minor negligence, which occurred over a limited period of time. As a result, this degree of negligence should be given some weight for fining purposes. In this respect, the EDPB noted that "[d]epending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral" (emphasis added).[164]

7.3. Action Taken by the Controller to Mitigate the Damage Suffered by Data Subjects (Art. 83(2)(c))

SATS has taken several remedial actions, at least with respect to most of the infringements.[165] For example, after Datatilsynet's inquiry, SATS has deleted the personal data of Complainant No 2, Complainant No 3 and Complainant No 4.[166] SATS has also updated its internal routines with the aim of ensuring a timelier handling of data subjects' requests.[167] Further, SATS noted that it will consider amending Section 5.2 of its general terms and conditions.[168] All in all, this goes to the credit of SATS and should be weighed in favor of the company in the present case.

7.4. Degree of responsibility of the controller taking into account technical and organisational measures implemented pursuant to Articles 25 and 32 GDPR (Art. 83(2)(d))

The criterion at Article 83(2)(d) is not applicable in the present case, as the infringements contested in the case at hand do not concern technical and organisational measures implemented pursuant to Articles 25 and 32 GDPR.

[163] See HR-2021-797-A, and Section 46 of the Public Administration Act ('forvaltningsloven').
[164] EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0, Adopted on 12 May 2022, para. 57.
[165] However, some instances of non-compliance are yet to be remedied, for instance by responding to the access request of Complainant No 1, and by updating the privacy policy and general terms of terms of service.
[166] See SATS' letter to Datatilsynet dated 28 April 2022.
[167] Ibid.
[168] Ibid.

7.5. Relevant Previous Infringements by the Controller (Art. 83(2)(e))

The criterion at Article 83(2)(e) is not applicable in the present case, as SATS has not been sanctioned for similar or otherwise "relevant" infringements in the past.

In its written representations, SATS argued that the absence of previous infringements should be considered a mitigating factor.[169] This argument should be rejected. In this regard, it suffices to note that, under EU/EEA law, it is well established that the absence of any previous infringement is a normal circumstance, which should not be taken into account as a mitigating factor.[170] Moreover, the EDPB has specifically noted that "[t]he absence of any previous infringements, […] cannot be considered a mitigating factor, as compliance with the GDPR is the norm. If there are no previous infringements, this factor can be regarded as neutral."[171]

7.6. Degree of Cooperation with the Supervisory Authority (Art. 83(2)(f))

SATS has responded to Datatilsynet's requests for information,[172] although it demanded several deadline extensions,[173] and SATS' cooperation did not go beyond what was required by law. Thus, in our view, this factor should be weighed neither in favor nor against SATS. As noted by the EDPB with respect to Article 83(2)(f) GDPR: "it would not be appropriate to give additional regard to cooperation that is already required by law".[174] This was not disputed by SATS in its written representations.[175]

7.7. Categories of Personal Data Affected by the Infringements (Art. 83(2)(g))

In light of the circumstances of the present case, the infringements committed by SATS do not appear to affect any special categories of personal data (within the meaning of Article 9 GDPR). However, some of them did affect information subject to a greater degree of sensitivity on the part of the individuals affected, such as data on their alleged wrongdoing. This element should be weighed moderately against SATS in the present case.

In its written representations, SATS argued that the factor in Article 83(2)(g) GDPR should be weighed in its favor.[176] The company claimed that the present case only affects "trivial data", and that the information on "alleged wrongdoing" was deleted in accordance with SATS'

[169] See SATS' letter to Datatilsynet dated 31 October 2022, p. 7.
[170] See e.g. Joined Cases T-305/94, T-306/94, T-307/94, T-313/94, T-314/94, T-315/94,T-316/94, T-318/94, T-325/94, T-328/94, T-329/94 and T-335/94, *LVM v Commission*, para. 1163; Case T-8/89, *DSM v Commission*, para. 317.
[171] EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0, Adopted on 12 May 2022, para. 94.
[172] See the Factual Background above.
[173] See email from SATS' Nordic Head of Legal & Compliance to Datatilsynet dated 27 October 2021; email from Brækhus Advokatfirma to Datatilsynet dated 31 March 2022; email from Brækhus Advokatfirma to Datatilsynet dated 19 April 2022; email from Advokatfirmaet Wiersholm to Datatilsynet dated 28 September 2022.
[174] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 14.
[175] Cf. SATS' letter to Datatilsynet dated 31 October 2022.
[176] Ibid, p. 7.

internal routines, and was thus not affected by the infringements identified by Datatilsynet.[177] This argument should be rejected. In this respect, it suffices to note that SATS kept its correspondence from 2019 with Complainant No 2 and Complainant No 3—which includes detailed information on their alleged misbehavior that led to their temporary ban from SATS' gyms—at least until 2021.[178] This is despite the fact that, as outlined above, SATS' retention policy provides that "If the customer relationship is terminated due to improper behavior from the member, name, date of birth and picture shall be kept for 60 months. Further, the member in question shall be marked as 'excluded'. The rest of the data shall be deleted, included possible reports on the behavior" (emphasis added).[179] Therefore, contrary to what SATS argued in its written representations, the information on "alleged wrongdoing" was not deleted in accordance with SATS' routines and is thus affected by the relevant infringements identified by Datatilsynet.

7.8. Manner in Which the Infringements Became Known to the Supervisory Authority (Art. 83(2)(h))

SATS' infringements in the present case became known to Datatilsynet as a result of several complaints submitted over a period of four years. This factor should be weighed against SATS.

In its written representations, SATS argued that this factor should not be weighed against SATS, as this would amount to a violation of the principle against self-incrimination.[180] Datatilsynet acknowledges that SATS was not required to report the infringements to us out of its own motion, and that the mere fact that a controller did not spontaneously report an infringement to Datatilsynet is not an aggravating factor. However, the negligent conduct of the controller before the relevant infringement(s) became known to the supervisory authority—which ultimately triggered the involvement of the authority in the case—"may also be considered by the supervisory authority to merit a more serious penalty".[181] In this case, the infringements were brought to the attention of Datatilsynet by several data subjects, after and due to the fact that SATS failed to remedy the identified instances of non-compliance, despite the fact that these data subjects have previously attempted to prompt SATS to comply. Thus, the infringements were brought to the attention of Datatilsynet as a result of SATS' failure to properly address the legitimate claims that various data subjects brought to its attention over the course of four years. This is the element that should be weighed against SATS in this case, and not the fact that it did not report the infringements to Datatilsynet of its own motion.

[177] Ibid.
[178] Excerpts from this correspondence were included by SATS in its replies to Datatilsynet dated 1 December 2021.
[179] In its correspondence with Complainant No 3 SATS also stated that such "rest of the data" would be deleted within 30 days. See email from kundeservice@sats.no to Complainant No 3 dated 11 October 2019 (attached to SATS' letter to Datatilsynet dated 1 December 2021).
[180] See SATS's letter to Datatilsynet dated 31 October 2022, p. 7.
[181] See Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 15.

7.9. Compliance with Corrective Measures Previously Ordered Against the Controller with Regard to the Same Subject-Matter (Art. 83(2)(i))

The criterion at Article 83(2)(i) is not applicable in this case, as no measures referred to in Article 58(2) GDPR have previously been ordered against SATS by Datatilsynet.

In its written representations, SATS argued that this factor should be weighted in favor of the company.[182] This argument should be rejected. First, the wording of Article 83(2)(i) GDPR makes clear that this factor applies only "where measures referred to in Article 58(2) have previously been ordered against the controller",[183] and no such measures have been ordered against SATS in the past. Secondly, the use of corrective measures is typically linked to the identification of an infringement and, as noted above (see Section 7.5), the absence of previous infringements—and hence of previous corrective measures—is a normal circumstance, which should not be taken into account as a mitigating factor.

7.10. Adherence to Approved Codes of Conduct or Certification Mechanisms (Art. 83(2)(j))

The criterion at Article 83(2)(j) is not applicable in this case, as SATS does not appear to adhere to any approved codes of conduct pursuant to Article 40 GDPR or approved certification mechanisms pursuant to Article 42 GDPR.

7.11. Any Other Aggravating or Mitigating Factor (Art. 83(2)(k))

Datatilsynet has not identified any other aggravating or mitigating factors in the present case. In this regard, it should be noted that, as outlined above, most of the complaints concern data subjects' requests and policies that predate the Covid-19 pandemic. Thus, the latter does not appear to have had any significant impact on the infringements. Moreover, the reduction of SATS' turnover due to the Covid-19 pandemic should not be considered a mitigating factor under Article 83(2)(k) GDPR.[184] This should be weighed neither against nor in favor of SATS in the present case.

In its written representations, SATS argued that some of the infringements concern facts that occurred in 2018 and 2019, shortly after the entry into force of the GDPR, and that this element should be weighed in SATS' favor.[185] We find this argument untenable. It suffices to reiterate that: (1) SATS has not responded to the access request of Complainant No 1 to this date, and it deleted the data of Complainants No 2 and No 3 only after the opening of Datatilsynet's inquiry in 2021, with the result that most of the violations identified by Datatilsynet were still ongoing in 2021; and (2) Datatilsynet's assessment of the lawfulness and transparency of SATS' processing has primarily focused on documents and policies that were still applicable in 2021 when we opened our inquiry. Furthermore, there were approximately two years between the

[182] See SATS' letter to Datatilsynet dated 31 October 2022, p. 8.
[183] See Article 83(2)(i) GDPR.
[184] EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 72.
[185] See SATS' letter to Datatilsynet dated 31 October 2022, p. 8.

entry into force of the GDPR in 2016[186] and the moment in which it started to apply in 2018.[187] Therefore, companies had at least two years to adapt to the new rules, and European supervisory authorities have repeatedly stated that there would be no "grace period" after the GDPR became applicable in 2018.[188]

Moreover, SATS argued that the length of the administrative proceedings is a factor that Datatilsynet should consider under Article 83(2)(k) GDPR, in particular to reduce the amount of the fine. In support of this argument, SATS noted that one of the complaints was submitted to Datatilsynet in 2018, and referred to several cases in which the Norwegian Privacy Appeals Board ("Personvernnemda") reduced a fine imposed by Datatilsynet due to an excessive duration of the case handling which—according to Personvernnemda—resulted in a violation of Article 6(1) of the European Convention on Human rights (ECHR).[189] In Datatilsynet's view, this argument should be rejected for the following reasons.

First, Personvernnemda has made clear that the duration of the administrative proceedings concerning the handling of a complaint should be calculated from the first request for information that Datatilsynet sent to the relevant controller,[190] and not from the moment Datatilsynet received the complaint.[191] This appears to be meant to follow the case law on the reasonable duration of criminal proceedings of the European Court of Human Rights ("ECtHR"), which found that the starting-point of the period to be taken into consideration is when the person affected by the investigation became aware of the charges against them or when they were substantially affected by the measures taken in the context of the investigation or proceedings.[192] In the present case, it is apparent that Datatilsynet first sent a request for information about Complaint No 1 to SATS on 23 March 2022[193] and notified SATS of its intention to issue an administrative fine on 26 September 2022. In other words, approximately six months elapsed before Datatilsynet notified SATS of its intention to issue an administrative fine. As for Complaints No 2, No 3 and No 4, it took Datatilsynet respectively approximately 1 year,[194] 11 months[195] and 6 months to notify SATS of its intention to impose an administrative

[186] See Art. 99(1) GDPR.
[187] See Art. 99(2) GDPR and § 32 personopplysningsloven.
[188] See e.g.: <https://www.theparliamentmagazine.eu/news/article/gdpr-no-period-of-grace-following-entry-into-force>; <https://www.natlawreview.com/article/happy-gdpr-day>.
[189] See SATS' letter to Datatilsynet dated 31 October 2022, p. 8.
[190] See PVN-2021-03 (stating (in Norwegian): "Nemnda legger for sin vurdering til grunn at forberedelsene med sikte på å avgjøre denne saken startet med tilsynets krav om redegjørelse").
[191] It should stressed the filing of a complaint does not invariably and automatically lead to the opening of an investigation.
[192] ECtHR, *Mamič v. Slovenia* (no. 2), App. No. 75778/01, judgment of 27 July 2006, paras. 23-24; ECtHR, *Liblik and Others v. Estonia*, App. Nos. 173/15 and 5 others, judgment of 28 May 2019, para. 94.
[193] See the Factual Background above.
[194] As noted in the Factual Background, the first request for information regarding Complaint No 2 was sent on 7 September 2021 and Datatilsynet notified its intention to issue an administrative fine against SATS on 26 September 2022.
[195] As noted in the Factual Background, the first request for information regarding Complaint No 3 was sent on 5 October 2021 and Datatilsynet notified its intention to issue an administrative fine against SATS on 26 September 2022.

fine.[196] Moreover, approximately four months elapsed between the date in which Datatilsynet notified SATS of its intention to issue an administrative fine and the date of the final decision.[197] Thus, the duration of the administrative proceedings was overall shorter than that of those cases reviewed by Personvernnemda—which SATS referred to in its written representations—which all lasted considerably more than one year.[198]

Secondly, when determining whether the duration of the proceedings has been reasonable, due regard must be had to factors such as the complexity of the case, the applicant's conduct and the conduct of the relevant authorities.[199] With respect to the first factor, the present case is relatively complex, given that the violations contested to SATS concern several provisions of the GDPR, and several complaints were handled jointly. Moreover, the procedure set out in Articles 56(1) and 60 applies to the present case, which entails additional procedural steps (compared to the cases reviewed by Personvernnemda and cited by SATS) and requires cooperation with foreign authorities. This adds to the complexity of the case.

As for the applicant's conduct, SATS contributed to the prolongation of the proceedings by asking for an extension of the procedural deadlines set by Datatilsynet essentially at each stage of the proceedings.[200] In total, SATS has asked for—and has been granted—deadline extensions for a time period of approximately two months.

As for the conduct of the relevant authorities, Datatilsynet has made efforts aimed at higher procedural efficiency, for example by handling the complaints jointly in a single procedure, rather than opening several parallel inquiries. Moreover, it should be noted that Datatilsynet is currently confronted with an exceptional backlog of cases,[201] and the ECtHR has found that in similar circumstances some delays in the proceedings are not unjustified.[202] For instance, in *Buchholz v. Germany*, the ECtHR came to the conclusion that the duration of the proceedings was not unreasonable also because it found that it could not "overlook the fact that the delays […] occurred at a time of transition marked by a significant increase in the volume of litigation".[203]

Thirdly, it should be noted that the ECtHR has almost never found that proceedings lasting less than two years violated Article 6(1) ECHR due to their excessive duration. In the overwhelming majority of cases where the Court found a violation of Article 6(1) the proceedings had lasted

[196] As noted in the Factual Backgound, the first request for information regarding Complaint No 4 was sent on 23 March 2022 and Datatilsynet notified its intention to issue an administrative fine against SATS on 26 September 2022.
[197] See Datatilsynet's letter to SATS dated 26 September 2022.
[198] Cf. PVN-2021-16; PVN-2021-03; PVN-2021-09.
[199] ECtHR, *Liblik and Others v. Estonia*, App. Nos. 173/15 and 5 others, judgment of 28 May 2019, para. 91.
[200] See email from SATS' Nordic Head of Legal & Compliance to Datatilsynet dated 27 October 2021; email from Brækhus Advokatfirma to Datatilsynet dated 31 March 2022; email from Brækhus Advokatfirma to Datatilsynet dated 19 April 2022; email from Advokatfirmaet Wiersholm to Datatilsynet dated 28 September 2022.
[201] The number of cases to be handled by Datatilsynet has been growing exponentially since 2018. Cf. Datatilsynet's Annual Reports <https://www.datatilsynet no/om-datatilsynet/arsmeldinger/>.
[202] ECtHR, *Buchholz v. Germany*, judgment of 6 May 1981; ECtHR, *Zimmermann and Steiner v. Switzerland*, judgment of 13 July 1983; ECtHR, *Foti and others v. Italy*, judgment of 10 December 1982.
[203] ECtHR, *Buchholz v. Germany*, judgment of 6 May 1981, para. 63.

four/five years or more.[204] This is further supported by legal literature on the ECHR case law on this subject matter, which notes how "a total duration of up to 2 years per level of jurisdiction in non-complex cases is generally regarded as reasonable".[205] For example, an investigation which lasted one year and eight months was not considered unreasonably long.[206]

Having regard to the above, the duration of the proceedings against SATS has not been unreasonable.

7.12. Conclusion with Regard to Whether to Impose an Administrative Fine

Having had due regard to the factors under Article 83(2), the infringements that have been identified warrant the imposition of an administrative fine in the circumstances of this case.

Despite the relative limited number of individuals affected by some of the infringements (i.e., the infringements connected to the rights of access and erasure) and the remedial actions taken by SATS, the reoccurrence of similar instances of non-compliance over an extensive period of time and SATS' approach towards the interpretation of its storage limitation, transparency and lawfulness obligations under the GDPR are indicative of systemic compliance flaws within the company, which—if not remedied—could result in important consequences for data subjects. In Datatilsynet's view, the imposition of an administrative fine is therefore warranted to produce a genuine deterrent effect, and dissuade SATS—as well as companies in general—from committing similar infringements in the future. Indeed, enforcement efforts must generate sufficient pressure to make non-compliance economically unattractive in practice.[207] This is particularly salient with regard to the kinds of infringements contested in the present case, as most of the administrative fines issued so far by European supervisory authorities concern the principles relating to processing of personal data; lawfulness of processing; valid consent; and transparency and rights of the data subjects.[208]

In its written representations, SATS claimed that the imposition of an administrative fine would be at odds with Datatilsynet's administrative practice regarding corrective measures, and hence with the principle of equal treatment. SATS claims that the imposition of a reprimand would be a more suitable measure in the present circumstances. In this respect, SATS referred to a prior case in which Datatilsynet imposed a reprimand against a company that failed to comply with some of its transparency obligations under the GDPR.[209] The latter case is, however, not

---

[204] Cf. European Commission for the Efficiency of Justice (CEPEJ), Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights (Council of Europe, 2018), pp. 112-122 <https://rm.coe.int/cepej-2018-26-en-rapport-calvez-regis-en-length-of-court-proceedings-e/16808ffc7b>.

[205] See Henzelin and Rordorf, 'When Does the Length of Criminal Proceedings Become Unreasonable According to the European Court of Human Rights?' 5(1) (2014) *New Journal of European Criminal Law* 79-109, p. 93.

[206] ECtHR, *Idalov v. Russia*, App. No. 5826/03, judgment of 22 May 2012, paras. 190-191.

[207] See Opinion of Advocate General Geelhoed in Case C-304/02, *Commission v. France*, delivered on 29 April 2004, para. 39.

[208] EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, pp. 33-34.

[209] See SATS' letter to Datatilsynet dated 31 October 2022, p. 9 (referring to Reprimand and Compliance Order - Mowi ASA, Doc. No 21/03656-12).

comparable with the present one, as it concerns only: (1) a failure to respond to a single access request on time due to the fact that such request ended up in the spam folder of the company's email inbox, a matter that was eventually amicably settled; and (2) a delayed provision of all of the information in Article 14 GDPR (which—contrary to Article 13—does not require that information be provided at the time of the processing, but within a month), which was eventually considered satisfactory by the relevant complainant.

At present, Datatilsynet has not handled other cases which may be deemed largely comparable to the present one. However, it should be emphasised that Datatilsynet has issued fines against other controllers too, including in circumstances where they had violated only some of the legal requirements violated by SATS and where such violations affected a single data subject.[210]

7.13. Calculation of the Amount of the Administrative Fine

Having had due regard to the factors under Article 83(1) and (2), we find an administrative fine of NOK 10 000 000 (ten million) to be appropriate in the circumstances of this case. This is for the reasons outlined below. In this respect, it should be noted that the setting of a fine is not an arithmetically precise exercise,[211] and supervisory authorities have a certain margin of discretion in this respect.[212] Nonetheless, they should indicate the factors that influenced the exercise of their discretion when setting a fine.[213]

In terms of the requirement under Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive, the financial position of SATS must be taken into account. The financial position of SATS is also relevant to determine the maximum fine applicable in the present case.

In 2021, SATS' total annual turnover appears to be of NOK 3 247 million.[214] Thus, the maximum fine applicable in the present case is EUR 20 000 000 (i.e., around NOK 200 000 000), as the latter amount is higher than 4% of the company's total annual turnover, and Article 83(5) provides that infringements of Articles 5, 6, 12, 15 and 17 GDPR shall be subject to "administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher" (emphasis added).

Having considered the above, a fine of NOK 10 000 000 (ten million) seems appropriate, as it represents approximately 5% of the maximum applicable fine and sits within the lower end of the spectrum of possible fines. Therefore, such a fine is commensurate with the seriousness of

[210] See e.g. Case 20/01874, Basaren Drift AS; Case 20/02220, Flisleggingsfirma AS; Case 20/02375, Ultra-Technology AS.
[211] See, *inter alia,* Case T-425/18, *Altice Europe NV v Commission*, para. 362; Case T-11/06, *Romana Tabacchi v Commission*, para. 266.
[212] See, *inter alia*, Case T-192/06, *Caffaro Srl v Commission*, para. 38.
[213] EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 75.
[214] See SATS Annual Report 2021, available at <https://satsgroup.com/wp-content/uploads/2022/03/SATS-ASA-Annual-Report-2021.pdf>.

the infringements for which it is imposed, taking into account all of the aggravating and mitigating factors outlined above (see sections 7.1-7.12 above).

Such a fine would represent approximately 0.3% of SATS' annual turnover for 2021. Therefore, it would have some significance to the company relative to its revenue—which is essential to ensure its dissuasive effect—without being disproportionate relative to the company's financial position and the infringements viewed as a whole.

The amount of the fine set out above takes into account that SATS' total annual turnover for 2021 decreased by 8% compared to 2020, primarily due to club closures and visit restrictions because of the Covid-19 pandemic.[215] While this is not a mitigating factor, Datatilsynet believes that the fine should be slightly adjusted in view of the difficult economic context in which the company is operating due to the pandemic.

For the sake of clarity, it should be noted that Datatilsynet has calculated the above fine on the basis of all of the infringements viewed as a whole, and has not cumulated separate fines for each of the individual infringements identified. In any event, given that all of the provisions violated by SATS may be fined up to 20 000 000 EUR, the total amount of the administrative fine has not exceed the amount specified for the gravest infringement, as demanded by Article 83(3) GDPR.

In its written representations, SATS claimed that the amount of the fine indicated above is disproportionately high and it would not be in line with the existing administrative practice across the EU/EEA regarding administrative fines.[216] In this respect, we reiterate that the setting of a fine is not an arithmetically precise exercise,[217] and supervisory authorities have a certain margin of discretion in this respect.[218] In any event, the cherry-picked selection of cases listed in SATS' written representations in support of its claim—none of which is entirely analogous to the present one—only focuses on the numeric value of the fines imposed, but does not show how each of the amounts relate to the economic size of the recipient of the fine.[219] The size of the undertaking concerned is one of the key elements that should be taken into account in the calculation of the amount of the fine in order to ensure its dissuasive nature.[220] Taking into consideration the resources of the undertaking in question is indeed justified by the impact sought on the undertaking concerned, in order to ensure that the fine has sufficient deterrent

[215] Ibid.
[216] See SATS' letter to Datatilsynet dated 31 October 2022, p. 10.
[217] See, *inter alia,* Case T-425/18, *Altice Europe NV v Commission*, para. 362; Case T-11/06, *Romana Tabacchi v Commission*, para. 266. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 74.
[218] See, *inter alia*, Case T-192/06, *Caffaro Srl v Commission*, para. 38. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 74.
[219] Cf. SATS' letter to Datatilsynet dated 31 October 2022, p. 10.
[220] EDPB, Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, paras. 405-412; EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 76.

effect, given that the fine must not be negligible in the light, particularly, of its financial capacity.[221]

Having regard to the above, a fine equal to 0.3% of SATS' annual turnover for 2021 is in line with fines issued in partially similar cases, including cases reviewed by Personvernnemda. In this respect, it suffices to note that in a case concerning violations of Articles 6(1) and 13 that Personvernnemda did not consider too serious, Personvernnemda deemed a fine equal to 0.9% of the annual turnover of the preceding financial year to be adequate.[222] Further, in a case concerning a serious violation of Article 6(1), Personvernnemda considered a fine equal to 7.9% of the annual turnover of the preceding financial year to be "not too high".[223] In this respect, it should be emphasized that SATS' infringements concern more provisions of the GDPR and affected more individuals compared to the latter two cases.

8. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, pursuant to Article 22(2) of the Norwegian Data Protection Act, the present decision may not be appealed before Personvernnemda. However, the present decision may be challenged before Oslo District Court ("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.[224]

Kind regards

Line Coll
Data Protection Commissioner

Luca Tosoni
Specialist Director

This letter has electronic approval and is therefore not signed

Copy to: Complainants; ADVOKATFIRMAET WIERSHOLM AS

[221] Case C-408/12 P, *YKK and Others v Commission*, para 85; Case C-413/08 P, *Lafarge v European Commission*, para. 104 and the case law cited therein. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 76.
[222] See PVN-2021-13.
[223] See PVN-2020-21.
[224] Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).