Datatilsynet

SATS ASA
Postboks 4949 NYDALEN
0423 OSLO

Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven § 24 første ledd 2. punktum

Your reference	Our reference	Date
	24/00844-10	20.08.2024

Final Decision - SATS ASA

1. Introduction and Factual Background

On 15 December 2023, the Norwegian Data Protection Authority (hereinafter "Datatilsynet", "we", "our", "us") received a complaint against SATS ASA (hereinafter "SATS") from the Swedish Authority for Privacy Protection (hereinafter "IMY") (Case 24/00844). The complaint was submitted by [redacted], a member of the fitness centers run by SATS in Sweden (hereinafter "complainant"), who essentially claimed that SATS violated Regulation (EU) 2016/679 (hereinafter "GDPR") as:

- SATS has unlawfully transferred personal data to a debt collection agency (Lowell Sverige AB, hereinafter "Lowell"), and has not informed the competent data protection authority about this.

- SATS has not responded to a request for erasure of his personal data transferred to Lowell that the complainant sent to SATS on 12 January 2023.

- SATS' privacy policy does not provide sufficient information, as it does not spell out exactly what personal data SATS processes and to which specific third countries such personal data may be transferred.

- With respect to the processing of personal data of SATS members in Sweden, the controller mentioned in the privacy policy is not the Swedish entity with whom the Swedish members have a contractual relationship.

Further to our inquiry, SATS informed us that, in January 2023, the complainant contacted SATS to inform them about an invoice that he incorrectly received from SATS' debt collection supplier (i.e., Lowell) and to request that all of his personal data processed in connection with the issuing of the invoice at hand be deleted.

The evidence produced by SATS shows that, in January 2023, SATS contacted Lowell to request them to annul the invoice at issue and to delete all personal data of the complainant. Furthermore, the evidence produced by SATS shows that, on 12 January 2023, SATS informed the complainant that the invoice had been annulled and that no payment was due, and offered him two months of free membership as a compensation for any inconvenience caused.

However, SATS acknowledged that it failed to properly inform the data subject about the deletion of his personal data. It noted that this was due to an occasional breach of its internal routines, which will be taken into account to improve SATS' routines in the future. SATS confirmed though that all personal data of the complainant have been deleted by Lowell, and that only a copy of the incorrectly issued invoice has been kept by SATS for mere bookkeeping purposes. On 27 February 2024, after we opened our inquiry, SATS informed the complainant about this.

SATS also informed us that it updated its privacy policy on 23 May 2023 (and again on 29 February 2024), after receiving on 6 February 2023 a fining decision that sanctioned SATS for several violations of the GDPR, including for violations of data subject rights and transparency requirements partially analogous to those mentioned in the complaint.[1]

Furthermore, SATS told us that it did not consider the transfer of personal data to Lowell as a reportable personal data breach under Articles 33 or 34 GDPR.

On 4 March 2023, the complainant wrote to IMY to inform them that, in his view, the action taken by SATS had not fully resolved the compliance issues identified in his complaint. The complainant also raised a few additional issues (e.g., an alleged lack of reply to an access request he submitted on 11 January 2023), which have not been dealt with as part of the present case, as they were not part of the original complaint. However, we trust that SATS will review all previous correspondence with the complainant to make sure that there are no responses that are still due to him.

2. Datatilsynet's Competence

Based on information provided by SATS in previous cases,[2] SATS runs a chain of fitness centers. It has its headquarter in Norway, but has also operations and offices in Denmark, Finland and Sweden.

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, such as the complainant. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

The SATS group has its main establishment (within the meaning of Article 4(16) GDPR) in Norway. Moreover, the processing of the personal data of SATS members, including the

[1] See Datatilsynet's decision No 20/02422-9 of 6 February 2023.
[2] Ibid.

complainant, qualifies as cross-border processing under Article 4(23) GDPR. This is because, 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 are the same in all of the European countries in which SATS operates.

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.

As a result, pursuant to Article 60(3) GDPR, a draft of the present decision was shared with the other supervisory authorities concerned, which did not raise any objections.

3. Datatilsynet's Assessment and Decision

With respect to the complainant's arguments on the lack of sufficient information in SATS' privacy policy regarding the kinds of personal data processed by SATS, it should be noted that listing all categories of personal data concerned is not required per se under Article 13 GDPR, whereas it is expressly required under Article 14 GDPR.[3] This is because the provision of information on the categories of personal data concerned is especially relevant when "the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained".[4] However, providing information on the specific categories of personal data processed may be necessary also when the personal data have been collected from the data subject to comply with the transparency principle in Article 5(1)(a) GDPR.

While it is true that, as argued by the complainant, SATS' privacy policy does not – and did not – spell out all kinds of personal data that SATS processes, it provides – and provided – several examples of personal data and categories of personal data concerned (e.g., name, gender, age, exercise history, health data, etc.). This may "avoid information fatigue".[5] Moreover, it should be noted that the personal data to be processed for issuing invoices (e.g., name, address, bank account details) do not include special categories of personal data and are typically obtained from the data subjects who are thus generally aware of them.

Therefore, the information provided in SATS' privacy policy about the kind of personal data processed by SATS does not appear to be insufficient to meet the GDPR's transparency requirements, at least with respect to the information to be provided to the complainant under Article 13 GDPR regarding invoicing and debt collection activities. To the extent that Article 14 GDPR is applicable, the fact that SATS did not spell out all the categories of personal data to be processed is a rather minor violation that we trust SATS will remedy by further updating its privacy policy. In this context, it should also be noted that the current version of SATS' privacy policy expressly states that personal data may be shared with Lowell:

[3] See Article 14(1)(d) GDPR.
[4] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, p. 36.
[5] Ibid., p. 7.

> In English: "We may also share information with other suppliers who act as data controllers, such as Lowell our debt collection partner."
>
> In Swedish: "Vi kan också dela information med andra leverantörer som agerar som behandlingsansvariga, såsom Lowell, vår partner för inkassotjänster".

As for the information on transfers of personal data to third countries, it is true that, as argued by the complainant, SATS' privacy policy (or at least the version in Swedish) in effect before the latest update in February 2024 did not provide any information on international data transfers.

This would be a clear violation of Article 13(1)(f) GDPR, if at that time SATS transferred personal data to third countries. However, this has not been investigated in the present case, given that the complainant's personal data have been transferred to an entity in Sweden (i.e., Lowell).

The current version of SATS' privacy policy states:

> In English: "We may transfer your personal data outside the EEA in certain situations, as some of our suppliers (or sub-suppliers) and business partners may be located in such countries. We will ensure that your data is secured by adopting appropriate safeguards to protect the privacy (such as EU's Standard Contractual Clauses). We will provide you with further details about such international data transfers upon request. If you want to obtain a copy of the safeguards, please use the contact details below."
>
> In Swedish: "Vi kan överföra dina personuppgifter utanför EES i vissa situationer, eftersom några av våra leverantörer (eller underleverantörer) och affärspartners kan vara belägna i sådana länder. Vi kommer att säkerställa att dina data är säkrade genom att anta lämpliga skyddsåtgärder för att skydda integriteten (såsom EU:s Standardavtalsklausuler). Vi kommer att tillhandahålla dig ytterligare detaljer om sådana internationella datatransferer vid begäran. Om du vill erhålla en kopia av skyddsåtgärderna, vänligen använd kontaktuppgifterna nedan."

This wording is insufficient to ensure full compliance with the transparency requirements set out in the GDPR. This is because "[i]n accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named."[6] However, the fact that the relevant third countries are not named in SATS' privacy policy is a rather minor violation that we trust SATS will remedy by further updating its privacy policy.

As for the transfer of the complainant's personal data to Lowell, we take note of SATS' argument that this was due to an occasional mistake affecting a single data subject, which – in

[6] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, p. 38.

their view – was unlikely to result in a risk to the rights and freedoms of natural persons, and was thus not a reportable personal data breach under Articles 33 or 34 GDPR. During the investigation, we found no evidence to dispute this conclusion. SATS was made aware of the mistake by the affected data subject himself – who was thus aware of it – and immediately took action to correct it and avoid any negative consequences for the data subject (e.g., undue payments). Moreover, the personal data at issue were transferred to one of SATS' regular suppliers – and not to an unknown third party – who promptly deleted the personal data concerned after having been notified of the mistake by SATS. Due to these facts this data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the competent supervisory authority or the concerned data subject was necessary. However, this data breach must be documented in accordance with Article 33(5) GDPR.[7]

In this regard, it should be noted that the transfer of personal data to a debt collection agency to pursue a debt on behalf of a controller does not generally give rise to specific data protection concerns, as the transfer may normally take place on the basis of Article 6(1)(b) or (f) GDPR.[8]

As to the complainant's argument that the controller mentioned in SATS' Swedish privacy policy was not the Swedish entity with whom Swedish members have a contractual relationship, we note that this fact is not in itself strange or problematic, as the controller does not necessarily need to be the local contractual counterparty, in particular where the local entity is part of a larger multinational group where decisions about personal data processing are taken centrally. In any event, after the latest update in February 2024, SATS privacy policy in Swedish now states that "SATS Sports Club Sweden AB" is the controller with respect to the processing of personal data of Swedish members:

> In Swedish: "SATS Sports Club Sweden AB ('SATS', 'vi', 'vår', 'oss') driver en kedja av gym och relaterade tjänster (såsom SATS Online, SATS-appen och SATS-webbplatsen). Denna integritetsnotis ger dig information om vår behandling av personuppgifter som ansvarig för personuppgifter."

We have not investigated as part of the present case whether this update reflects today's factual reality regarding decision-making on means and purposes of personal data processing. However, we understand that, at least in the past, decisions on means and purposes of the processing of personal data in all of the countries where SATS operates were entirely or at least partially made in Norway. We would thus encourage SATS to review this to make sure that what is indicated in the Swedish privacy policy reflects the actual allocation responsibilities and decision-making within the SATS group.

With respect to the complainant's erasure request, SATS itself has acknowledged that it did not appropriately respond to such a request. Indeed, SATS failed to provide information on the action taken on the request without undue delay and in any event within one month of receipt of the request, in violation of Article 12(3) GDPR. However, this may be considered a relatively minor violation, as SATS did take action on the request; it only failed to properly inform the

[7] See by analogy EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Adopted on 14 December 2021, Version 2.0, paras. 114-118.
[8] See, e.g., the judgment of Administrative Court of Mainz of 20 February 2020 (VG Mainz - 1 K 467/19.MZ).

data subject about it. Moreover, SATS has eventually provided information on the action taken to the data subject on 27 February 2024, although it did so in Norwegian. Even though Scandinavian languages are generally mutually intelligible, communications with data subjects should normally occur in their language to ensure that the communication is provided in "clear and plain language" as required by Article 12(1) GDPR. We trust that SATS will take note of this for any future communication with data subjects.

Finally, it should be noted that the violations identified in the present case have taken place before SATS was fined for partially similar violations on 6 February 2023.[9] Therefore, they were presumably linked to the systemic compliance issues for which SATS has already been fined in our decision of 6 February 2023, which has led SATS to upgrade its data protection policies and routines.

In light of the above, Datatilsynet is of the view that, despite the rather minor violations identified, it is not necessary to adopt any corrective measures against SATS in the present case. In this respect, it should be noted that there is no obligation on supervisory authorities to impose corrective measures in all cases or when the complainant so requests.[10] Nonetheless, we trust that SATS will take note of and remedy all violations identified by updating its data protection policies and routines.

However, this decision is without prejudice to the possibility of opening future inquiries into SATS' compliance with data subject rights, and the lawfulness and transparency requirements set out in the GDPR, including with respect to the updates to its privacy policy that SATS is expected to undertake in light of the present decision.

4. 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.[11]

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

[9] See Datatilsynet's decision No 20/02422-9 of 6 February 2023.
[10] See Opinion of Advocate General Pikamäe in Case C-768/21, TR v Land Hessen.
[11] Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

This letter has electronic approval and is therefore not signed