Summary Final Decision Art 60

Complaint

EDPBI:NO:OSS:D:2023: 665

Violation identified ; Administrative fine

Background information

Date of final decision:	06 February 2023
Date of broadcast:	20 February 2023
LSA:	NO
CSAs:	FI, DK, SE.
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 6 (Lawfulness of processing), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 15 (Right to access by the data subject), Article 17 (Right to erasure ('right to be forgotten')).
Decision:	Violation identified, Administrative fine.
Key words:	Lawfulness of processing, Transparency, Right to erasure, Right to rectification, Data subject rights.

Summary of the Decision

Origin of the case

The inquiry focused on the controller's compliance with Articles 5, 6, 12, 13, 15 and 17 GDPR in connection with the complaints against it lodged with the NO SA between 2 October 2018 and 8 December 2021. All such complaints concerned alleged infringements of data subjects' rights committed by the controller, in connection with its handling of data subjects' requests submitted pursuant to Articles 15 and 17 GDPR. In the **first complaint,** the complainant claimed that the controller had transferred the personal data to other companies within its corporate group, as well as to Facebook outside the EU/EEA, without a proper legal basis. The complainant claimed also that an access request submitted on 29 August 2018 pursuant to Article 15 GDPR had remained unanswered. In the **second complaint**, the complainant claimed that the controller had failed to respond to an access request submitted on 25 February 2019 pursuant to Article 15 GDPR and that it had refused to comply with an erasure request submitted on the same date pursuant to Article 17 GDPR, after the membership to the fitness centre run by the controller was terminated by the controller. In the **third complaint**, the complainant claimed that the controller had refused to comply with an erasure request submitted on 5 October 2019 pursuant to Article 17 GDPR, following the termination of the membership by the controller. In the **fourth complaint**, the complainant claimed that the controller

had refused to comply with an erasure request regarding their training history submitted on 6 August 2021 pursuant to Article 17 GDPR.

Findings

In the first place, the NO SA found that, by failing to timely act upon two separate access requests, the controller had infringed **Articles 12(3) and 15 GDPR.** The NO SA stated that 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.

In the second place, the NO SA found that, by failing to take prompt action and erase certain personal data without undue delay pursuant to three separate erasure requests, the controller had infringed **Articles 5(1)(e), 12(3) and 17 GDPR.** For two of the erasure requests, the original purpose of processing had been to enforce the exclusion of banned members. However, the controller retroactively stated that the purpose of the storage is to be able to process the information in connection with the ban and that this purpose does not expire as soon as the ban is lifted. It also claimed that such a change of position on the purpose would not affect the assessment of the legitimacy of the retention period. The NO SA emphasized that it is not possible to adjust the relevant purpose *ex post*; the assessment of retention should be made with respect to the purpose identified by the controller at the outset of the relevant processing. In the third erasure request, the complainant withdrew their consent to storage of their training history as the controller's terms and conditions stated that they were entitled to. The controller stated that the legal basis was not consent and that it could retain the personal data for a period of six months in light of the ongoing pandemic. The NO SA found that a storage period of six months was not justified and that in any case, the controller retained the personal data in question for longer than six months.

In the third place, the NO SA found that, 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, the controller had **infringed Articles 5(1)(a), 12(1) and 13 GDPR.** The controller has established a specific data retention policy with respect to the personal data of members whose membership is terminated by the controller. Nonetheless, no publicly available documents provide specific information on the retention period at hand. In the view of the NO SA, the controller violated Articles 5(1)(a) and 13(2)(a) GDPR as it failed to ensure transparency about legal bases, the period for which it stores the personal data of banned members and/or the criteria used to determine that period. It is not sufficient to inform data subjects about the retention period when the controller notifies them of the termination of their membership.

Lastly, the NO SA found that, by failing to rely on a valid lawful basis to process the training history data of the members of its fitness centres, the controller had infringed **Articles 5(1)(a) and 6(1) GDPR.** The privacy policy simply stated that the controller's 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. The terms and conditions stated that processing of training history was based on consent. The consent to the processing of training history data tied to the acceptance of the controller's general terms and conditions is invalid. Neither Article 6(1)(a) nor Article 6(1)(b) was a valid legal basis for the controller's processing of training history data as the consent to such processing was not "freely given" and "informed", as it was tied to the general acceptance of the controller's terms and conditions, and in any event the processing was not objectively necessary to the performance of the membership contract.

Decision

The NO SA found that the controller had infringed **Articles 5, 6, 12, 13, 15 and 17 GDPR** in handling the data subjects' requests submitted pursuant to Articles 15 and 17 GDPR.

Pursuant to Article 58(2)(i) GDPR, the NO SA issued an administrative fine of NOK 10 000 000 (ten million) against the controller.