Summary Final Decision Art 60

Complaints

Violation identified, Administrative fine.

EDPBI:LSA:OSS:D:2022:627

Background information

Date of complaint:	22 May 2018
Draft decision:	18 October 2022
Revised draft decision:	08 December 2022
Date of final decision:	27 December 2022
Date of broadcast:	27 December 2022
Controller:	[redacted]
Processor:	N/A
LSA:	FI
CSAs:	AT, IT, BE, CZ, FR, DK, EL, DE, HU, NL, NO, SK, SL, SE, LU, ES, PL
Legal Reference(s):	Article 4 (Definitions), Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), Article 7 (Conditions for consent), Article 9 (Processing of special categories of personal data), Article 13 (Information to be provided where personal data are collected from the data subject), Article 45 (Transfers with an adequacy decision), Article 46 (Transfers by way of appropriate safeguards), Article 49 (Derogations for specific situations)
Decision:	Violation identified, Administrative fine.
Key words:	Health records, Data subject rights, Lawfulness of processing, Consent, Administrative fine.

Summary of the Decision

Origin of the case

Between 22 May 2018 and 18 February 2019, five complaints concerning the controller were lodged with the LSA. A complaint lodged with the Austrian SA was transferred to the LSA so to handle the case jointly with the other five complaints. According to the complainants, the use of a heart rate monitor manufactured by the controller required the use of the controller's service and acceptance of the controller's Terms of Use and Privacy policy to which the complainants did not wish to consent. In order to use the service, the complainants had to give their consent to the following processing

operations: processing of personal data concerning the heart rate; transferring personal data outside the EU/EEA. The controller's Terms of Use stated the following, among other things: "By saving, submitting, or transferring content to the controller's services, you are granting an uncompensated, global, transferable, sub-licensable right to use, reproduce, present in public, edit, translate, and share your User Content. Excluding the rights related to your personal data, the rights you have granted to the controller are irrevocable." The controller's service was also offered in other EU/EEA Member States and the processing of personal data was subject to similar conditions, irrespective of the country in which the user was located. In addition to complaints, the LSA had, on its own initiative, initiated to investigate the processing of research and product development described by the controller in its Privacy Notice. According to the response given by the controller, the controller processed the personal data of users on the basis of a legitimate interest for research and product development purposes. The controller had also emphasised that the data was anonymous.

Findings

The LSA found that the controller had been obliged to request explicit consent to the processing of heart rate data on the basis of Article 9(2)(a) of the GDPR. The controller had not been obliged to inform about the processing of personal data in accordance with Article 13 of the GDPR when purchasing a heart rate device. In addition to the heart rate data, the controller also processed other data concerning the health of the data subject, when the controller was processing maximum oxygen uptake and the body mass index. The consent requested by the controller to the processing of other data concerning health had not been in compliance with the GDPR, and therefore the controller had not had a legal basis for processing other health-related data in accordance with Article 9(2) of the GDPR. At the time when the complaints were lodged, the controller had grounds to transfer data to the United States. The consent collected by the controller to the processing of user content did not comply with Article 4(11) of the GDPR and it did not meet the conditions for consent laid down in Article 7(2) and (4) of the GDPR.

Decision

The LSA ordered the controller to bring the consent collected for the processing of maximum oxygen uptake and the body mass index into compliance with the GDPR within three months for new data subjects, and within six months for existing data subjects from the date of receipt of the decision. The LSA ordered to assess whether, in addition to heart rate data, maximum oxygen uptake and the body mass index, the controller processed other health data belonging to special categories of personal data when combining user-related data in the controller's service. Where the controller processed data belonging to special categories of personal data, the controller had to ensure that it had consent under the GDPR to the processing of all data relating to health that it processed. The LSA also ordered to ensure, without delay of the date of receipt of the decision, that the controller had a legal basis pursuant to Article 6(1) of the GDPR to process personal data in connection with "user content".

The LSA issued a reprimand to the controller under Article 58(2)(b) of the GDPR, as the consent requested by the controller to process the maximum oxygen uptake and the body mass index had not been in line with the GDPR. The controller had not had a legal basis for the processing of personal data that are an integral part of the controller's core business activity, which included the processing of data concerning health.

The LSA also imposed an administrative fine according to Article 83 of the GDPR. The controller infringed a provision under Article 83(5)(a) of the GDPR (Article 9). The infringement has thus concerned a violation of a higher category of administrative fine. The controller's turnover for 2021 was [redacted]. The LSA ordered the controller to pay an administrative fine of EUR 122 000 to the State under Article 58(2)(i) and Article 83 of the GDPR. The LSA considered the administrative fine of EUR 122 000 to be effective, proportionate and dissuasive.