OFFICE OF
THE DATA PROTECTION OMBUDSMAN

Notice: This document is an unofficial translation of the Data Protection Ombudsman's final decision (national record no. 1198/161/2022, IMI case no. 50199). Only the Finnish version of the decision is deemed authentic.

Record no. 1198/161/2022

IMI Case no. 50199

27 December 2022

Referring to complaints under national record numbers: 1875/452/2018, 2123/182/2018, 2405/182/2018, 3194/182/2018, 4318/146/2018, 1456/182/2019

# Final decision of the Data Protection Ombudsman and the Collegial Body for Sanction

## Case

Processing of personal data in connection with the [redacted] service

## Controller

[redacted]

## Case background

1. Between 22 May 2018 and 18 February 2019, five complaints concerning [redacted] (*hereinafter:* "[redacted]" or **"controller**") were lodged in the Office of the Data Protection Ombudsman. Complaints concern [redacted] service (*also:* "[redacted]" or "[redacted]").

2. During the abovementioned period, a complaint was lodged in the Austrian supervisory authority concerning the processing of personal data by the controller in [redacted] service. Given that the processing of personal data at issue has or is likely to have a significant effect on data subjects located in other Member States of the European Union, the matter must be processed in the cooperation mechanism according to Article 60 of the General Data Protection Regulation (*hereinafter:* "**GDPR**"). The Data Protection Ombudsman is deemed to be the lead supervisory authority regarding these personal data processing activities carried out by the controller. Hence the complaint lodged with the Austrian supervisory authority was transferred to the Office of the Data Protection Ombudsman on 18 July 2018. The case will be handled jointly with the other five complaints.

3. The Data Protection Ombudsman processes the complaints lodged by the complainants (*hereinafter:* also "**complainants**") jointly, on the basis of section 25 of the Administrative Procedure Act (434/2003).

## Content of the complaints

4. According to the complaints, the use of a heart rate monitor manufactured by the controller requires the use of [redacted] service and acceptance of [redacted]'s Terms of Use and Privacy

policy to which the complainants did not wish to consent. In order to use [redacted] service complainants must accept i.e., give their consent to the following processing operations:

i. processing of personal data concerning the heart rate by ticking a box that states the following: *"I agree that [redacted] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [redacted] Privacy Notice. I can change my settings about this consent at any time.";*

ii. transfer of personal data outside the EU/EEA by ticking a box that states the following: *"I agree that my personal data may be transferred and processed outside my country of origin as described in the [redacted] Privacy Notice. I can change my settings about this consent at any time."*; and

iii. [redacted]'s Terms of Use that state the following, among other things: *By saving, submitting, or transferring content to [redacted] services, you are granting [redacted] 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 [redacted] are irrevocable. Please note that even after you have closed your user account and your personal data has been deleted from [redacted] systems, material such as comments posted on discussion forums will not be removed. However, before closing your account, you can always remove User Content you have submitted to the services, including any comments posted."*[1]

## Cross-border nature of the matter

5. [redacted] service is also offered in other EU/EEA Member States and the processing of personal data is subject to similar conditions, irrespective of the country in which the user is located. Since the processing of personal data which takes place in the context of the activities of a single establishment of a controller in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State, the case must be regarded as cross-border character within the meaning of Article 4(23) of the GDPR.

6. The case is therefore dealt within the context of a 'one-stop shop' mechanism in accordance with Article 60 of the GDPR.

7. According to an assessment of the matter, decisions concerning the purposes and means of the processing of personal data related to [redacted] are made in Finland, which is why the Office of the Data Protection Ombudsman is the leading supervisory authority referred to in Article 56 of the GDPR.

8. The Office of the Data Protection Ombudsman will deal with the matter in accordance with the procedure laid down in Article 60 of the GDPR in cooperation with the supervisory authorities of the participating Member States. In the present case, the concerned supervisory authorities (*hereinafter also:* "**CSAs**") within the meaning of Article 4(22)(b) of the GDPR are the supervisory authorities of Italy, Belgium, the Czech Republic, France, Denmark, Greece, Germany, Hungary, Netherlands, Norway, Slovakia, Slovenia, Sweden, Luxemburg, Spain and Poland, since the processing affects or is likely to significantly affect data subjects in these Member States. The Austrian Supervisory Authority is a supervisory

[1] Extract from [redacted]'s Privacy Notice dated 22 May 2018

authority concerned on the basis of Article 4(22)(c) of the GDPR as it has received a complaint.

## Proceedings in the cooperation mechanism

9. In accordance with Article 60(3) of the GDPR, the Office of the Data Protection Ombudsman as the lead supervisory authority, has provided relevant information on the matter to the CSAs.

10. The Office of the Data Protection Ombudsman has communicated controller's response to the CSAs[2]. In addition, the Office of the Data Protection Ombudsman has reserved the CSAs an opportunity to present observations on written request for hearing of views and request for clarification before sending written request for hearing of views and request for clarification to the controller. Of the CSAs, the French Supervisory Authority (The Chair of the Commission Nationale de l'Informatique et des Libertés, *hereinafter:* "**CNIL**") has provided comments to the Office of the Data Protection Ombudsman. The comments on written hearing concerned, inter alia, the following:

    i. CNIL has drawn attention to the controller's response to the request for additional clarification 19.11.2019, in which the controller has stated that it processes information about the *length of the user, weight, age, training background, active orientation and sleeping goal*. CNIL has considered that it should be assessed whether the controller also processes other data belonging to special categories of personal data if it is able to combine the data collected. Also, CNIL has stated that information provided by the controller regarding the processing of special categories of personal data processed by the controller has not been clear.

    ii. CNIL has also drawn attention to the processing of personal data concerning research and product development carried out by the controller.

11. As explained above, the Data Protection Ombudsman has already tried, before drafting a draft decision pursuant to Article 60(3) of the GDPR, to hear CSAs views on the preliminary assessment of the Data Protection Ombudsman.

12. The observations made by CNIL have been taken into account as follows:

    i. Following the observation made by CNIL, a question has been added to written request for hearing of views and request for clarification on whether the controller processes other special categories of personal data.

    ii. As the processing of personal data for research and product development purposes has not been the subject of complaints, the question concerning research and product development will not be dealt in the context of this decision. The case may be declared admissible on its own initiative at a later stage. In this context, the Data Protection Ombudsman notes that when registering for [redacted], it is currently possible to object to the processing of personal data for this purpose[3].[4]

[2] Controller's response to the request for clarification 9 November 2018 and additional request for clarification 19 November 2019.
[3] [redacted]'s website, visited on 1 May 2022
[4] See also paragraph 101 of the decision

13. The draft decision of the Data Protection Ombudsman and the Collegial Body for Sanction has been submitted to the CSAs on 18 October 2022 in accordance with Article 60(3) of the GDPR. The CSAs has been required to submit a relevant and reasoned objection pursuant to Article 4(24) of the GDPR to the draft decision of the Data Protection Ombudsman and the Collegial Body for Sanctions by 18 November 2022.

14. On 18 November 2022 CNIL submitted a relevant and reasoned objection to the draft decision of the Data Protection Ombudsman and the Collegial Body for Sanctions. In its objection, CNIL is of the opinion that the Data Protection Ombudsman should exercise corrective powers provided for in Article 58(2) of the GDPR as a result of infringements of Article 7(2) and (4) of the GDPR[5].

15. In addition to the objection, CNIL has submitted a comment on the draft decision. In its comment, CNIL proposes that the Data Protection Ombudsman associates its order under Article 58(2)(d) of the GDPR for the infringement of Article 9[6] with a deadline the company must respect to comply with the GDPR.

16. The Data Protection Ombudsman has taken the objection raised by CNIL into account in its decision and added an order for infringement of Article 7 of the GDPR. The Data Protection Ombudsman has also taken into account the comment submitted by CNIL. Following the CNIL's objection, the amendments to the draft decision of the Data Protection Ombudsman were dealt with the Collegial Body for Sanctions on 8 December 2022.

17. None of the CSAs has within a period of two weeks expressed a relevant and reasoned objection to the revised draft decision. The deadline for objection has been 23 December 2022. Therefore, according to the Article 60(6) of the GDPR the lead supervisory and the CSAs are deemed to be in agreement with the revised draft decision and shall be bound by it.

## Response received from the controller

18. The Office of the Data Protection Ombudsman requested clarification from the controller on 18 October 2019 and 4 November 2019. The controller submitted a response to the requests on 9 November 2018 and 19 November 2019. In its responses the controller submitted the following details, among others.

### General information about [redacted]'s heart rate monitors and [redacted] service

19. The controller has provided the following general information about [redacted] service:

*"The [redacted] service and [redacted]'s devices (wrist devices, sensors) are two separate things. When purchasing a [redacted] product, the customer does not automatically gain access to the [redacted] service. The majority of our devices require the use of the [redacted] service, some devices can be used completely or to some extent without the service. This information is shown on the packaging and in the instructions of devices. Information on the matter can also be found on our website.*

*One of the key principles with regard to [redacted]'s devices and services is that the devices (wrist devices and sensors) are used to collect data (e.g. heart rate, activity data and location data during sports activity) and the collected data is transferred to the [redacted] service for analysis in order to provide various added-value services. Although the basic functions of certain devices can be used*

[5] See paragraph 102 v of the decision
[6] See paragraph 103 i of the decision

*on their own, without the [redacted] service (so-called stand-alone use), use of the service is required in order to get the best added value.*

*The [redacted] service is free of charge but requires the user to sign up, accept the terms of use and give the required consent.*

*The complaints submitted to the Office of the Data Protection Ombudsman criticise the fact that a registered user must consent to [redacted]'s use of the customer's personal data and that the service promised when purchasing a [redacted] heart rate monitor cannot be used without giving this consent. However, the device and the service are in fact two separate things and the service is not "sold" in connection with the purchase. Instead, use of the service is recommended - and in some cases required. In the latter case (use of the product requires use of the service), the customer is informed about the service being required on the product packaging, among other places. However, there are separate terms of use for the service, which the customer must consent to before using the service. As stated above, we also offer customers who have purchased a device the opportunity to return the product if the customer is not ready to agree to the terms of the [redacted] service when creating a user account."*

20. The controller has further specified [redacted] service as follows:

*"The basic functions of the monitor include "setting the basic data of time and user (length, weight, date of birth, exercise background, activity target, sleeping goal). It is also possible to attach a separate heart rate sensor into the wrist device without [redacted] account. The basic functions include measuring the causes, activity and exercise with default profiles, such as running, walking and cycling. Depending on the activity, basic functions enable, for example, the measurement of heart rate, consumed calories, speed, training trips, tours and duration of the exercise. The device can also use timer and an alarm function. You can also change your user interface visually by selecting a lockboard of your choice. The amount of basic functions varies by type of equipment, and the properties of the device may enable, for example, breathing exercises.*

*In stand-alone use, the software of the device cannot be upgraded for the time being without the [redacted] code, but the device can be put into use and its basic functions can be used with the software installed on the device and that is available on the device when the customer buys the device. Of course, this software also includes all the functions available through the [redacted] service, but it is not possible to use them in stand-alone mode. These additional functions include various graphics and controls that require algorithms and platforms in the [redacted] service."*

## Consent as a legal basis for the processing of personal data

21. The controller has stated the following:

*"In May 2018, along with many other companies, [redacted] also made changes to its legal documents due to the new data protection regulation. We rewrote documents, such as our Terms of Use and Privacy Notice, into a more user-friendly form. The actual Terms of use did not change much, and all changes were made for the advantage of the user."*

22. The controller has stated that it has completely changed the grounds for processing due to the following factors:

*"There were various reasons for changing the legal basis. The first reason was legislation outside the EU. As stated above, [redacted] is a global company with customers all over the world. Thus, [redacted] must also comply with the data protection laws of countries outside of the EU area. [redacted] At present, we can only offer the [redacted] service in one form (which is the same to everyone) around the world and can therefore not customise the principles related to the operation and use of the service on a country-specific*

*basis. We are currently looking into technical prospects for country-specific operation and use, which would take into account the unique features of each country and could help optimise this aspect of registration, but we are currently unable to offer such functionality.*

[redacted] *According to EU's interpretation, data based on heart rate combined with a user's other data (height, weight, age) is comparable to health data. This data can be used to draw conclusions on the person's health. Because the operation of the* [redacted] *service is largely based on the use of this type of data, we are directly compelled by law to use consent as the legal basis for collecting heart rate data from our customers.* [redacted]

*The third reason for changing the legal basis was our desire to ensure that our customers truly understand the principles and practices used for processing their personal data. We wanted to make it clearer to our customers how we process their data. This primarily relates to customer service. We believe that some of our customers had not actually read our terms of use and privacy policy with sufficient care before agreeing to them, and we wanted to draw their attention to what is done to their data and how it is use. The submitted complaints have in fact shown that our concerns were well-founded. Nothing has changed in the actual processing of data."*

23. In its response, the controller has described the collection of consent process as follows:

*"Consent and new customers: When a new customer purchases a* [redacted] *device, the customer is instructed to sign up for the* [redacted] *service in order to gain full benefits from the device. However, use of the service is not mandatory and is not an automatic part of acquiring a device. If a new user does not wish to give the required forms of consent when registering into the* [redacted] *service, the customer can decide not to use the service and no data on the customer will be saved into* [redacted] *'s systems. No data on the customer is recorded into the* [redacted] *service before the customer has given the requested consents. If a customer decides to not agree to the terms of the* [redacted] *service and refuses to give the requested forms of consent, the customer is also entitled to return the device to the place of purchase and be refunded. However, it should be noted that, in accordance with our current policy, it must be possible to set up and use the basic functions of our wrist devices without signing up to the* [redacted] *service. Set up and use without the service is possible with devices such as devices brought to the market in the autumn of 2018* [redacted] *and some devices that were already on the market.*

*Consent and old customers: When an old user first signed up to our service, the user agreed to our terms of use and privacy policy valid at the time of signing up. It was not possible to create a* [redacted] *without the acceptance of these documents. By agreeing to the terms, the user gave his/her consent to the collection of the user's data and any transfer of the data outside the EU/EEA. When* [redacted] *implemented changes to the legal basis for the processing of personal data, changing the basis from contract to consent, only the legal basis for processing sensitive data changed, not the actual processing of personal data. Thus, our old users have already given their consent to the same practices, only the legal basis has changed. If an old user does not wish to give his/her consent to these same practices on the new legal basis, we interpret this as the user having withdrawn his/her agreement to the Terms of use and Privacy policy which the user has previously agreed to, which in turn entitles us to terminate the user's contract and the use of the service. If a user does not wish to give his/her consent, the* [redacted] *account of the user will be locked and the user will have six months to change his/her mind, give his/her consent and continue the use of the service. After six months, the account and all data connected to it will be erased. For this entire six-month period, the user may exercise his/her legal right to transfer the data and may download the data using* [redacted] *'s account management service (*[redacted]*). A user may delete their own account or request the deletion of his/her account, in which case the account will be deleted within 30 days."*

24. The controller further states the following:

> *"The controller is aware of the difficulties related to the use of consent in this respect and we did not decide upon it lightly. However, due to reasons related to countries outside the EU, we felt that we did not have any other option. And as stated above, the EU General Data Protection Regulation also requires us to ask for consent for the processing of our customers' heart rate data. We have made no changes to the processing of data itself and our old customers are not being forced to agree to anything they have not agreed to previously. This is in compliance with Article 7 of the GDPR, and customers always have the choice of whether or not they want to use our service."*

25. In its response, the controller has referred to the decision (Decision 16 October 2018 Case Reference Number RFA0755227) issued by the UK Supervisory Authority (Information Commissioner's Office, *hereinafter* "**ICO**"). According to the controller, ICO has unambiguously stated in its decision that the controller's procedure complies with data protection obligations.

26. On 13 May 2022, the Office of the Data Protection Ombudsman requested the controller to submit the ICOs decision referred to in paragraph 25. The controller submitted ICO's decision on 20 May 2022.

27. ICO's decision to which the controller referred has concerned a complaint received by ICO in spring 2018. The complaint concerned the fact that the controller has required the complainant concerned to give their consent to the use of [redacted], even though the complainant has been a user of the [redacted] service for several years. As a result of the complaint, ICO has requested clarification from the controller.

28. In its clarification request, ICO has asked the controller to provide an explanation of why the controller has decided to request consent for the processing of personal data and what has led to a change in the grounds for processing. In addition, ICO has requested explanations as to why consent has also been required from old users whose personal data have already been processed by the data controller.

29. In the response submitted to ICO, the controller has told that when the GDPR became applicable, the biggest change in the controller's operations was changing the legal basis for processing from contract to consent. The controller has also been obliged to ask old users for consent to the processing of personal data, the transfer of data and the processing of sensitive personal data. The controller has explained that the processing of personal data in itself has not changed, but only old users have been asked to give their consent to the processing of personal data due to the requirements of the GDPR.

30. On 16 October 2018, ICO submitted a reply to the controller where ICO has stated that, in the light of the clarification provided by the controller, ICO welcomes the steps taken by the controller in relation to the change in the basis of processing based on consent and that the actions of the controller are in line with the GDPR. ICO has also stated that it does not consider it necessary to examine the controller's activities more extensively in terms of the grounds for processing.[7]

---

[7] ICO's response of 16 October 2018: *"In light of the information you have provided, we are satisfied that [redacted]'s actions relating to the change in lawful basis for processing to account on consent, is in compliance with your data protection obligations. As such we do not request any further information from you, nor do we intend to take any further action in relation to the complaint raise by [redacted]."*

31. The Data Protection Ombudsman draws attention to the fact that the response submitted by the controller to ICO is equivalent to that provided by the controller to the Office of the Data Protection Ombudsman (see paragraphs 21 to 24 of this decision).

### Disclosure of personal data to third parties

32. In its clarification, the controller states that the concepts "disclosure" and "transfer" are easily confused. On the disclosure of data, the controller stated the following:

*"[redacted] never discloses the data to third parties. This is included in our Privacy Notice: [redacted] never discloses any of your personal information without a separate permission from you, unless it is necessary for handling your order, carrying out your request, or managing our interactive customer programs. Information may, however, be disclosed if necessary because of law, a court order, or a regulation or request issued by authorities."*

### Transfer of data outside the EU/EEA

33. With regard to the transfer of data, the controller has stated, among other things, the following:

*"[redacted] transfers some data to outside the EU/EEA. Almost all [redacted] service user data is stored on servers located within the EU (Finland and Ireland). However, [redacted] does use a customer email service provider with a server located in the United States. We also use a service monitoring service provider with a server located in the United States. In both cases, it is possible that a user's email address or user ID is transferred to the service provider's server. These data storage locations have been the same as long as the [redacted] service has existed, and customers have been informed about data transfer in our Privacy Policy before May 2018 and in our Privacy Notice after May 2018.*

*Data transfer is subject to Article 49(1)a of the GDPR. In addition to the consent given by the user, we also adhere to safeguards put forward in Article 46. We conclude a data processing contract with every service provider we use. In order to ensure safe transfer and processing of data, we conclude a contract based on EU's standard contractual clauses with any service provider located outside the EU/EEA, located in a country that the EU deems to not have an adequate level of data protection or not certified with the EU-U.S. and Swiss-U.S. Privacy Shield.*

*Our customers, both old and new, have been informed about the transfer of data to outside their own country. We have used the same practice for the entire existence of the [redacted] service, and we have always informed our customers about this practice. We have noticed from customer contacts received by our customer service, that many of our customers have become more aware of the practice since we have started requesting a separate consent for data transfer. Increasing awareness has been one of our goals. According to our view, making our customers aware of the matter shows that our practice is in compliance with the GDPR. We help our customers to better understand what is done to their data. This seems to have come as a surprise to some of our customers, even though we have informed them about the practice before."*

### User content

34. The controller has provided, among other things, the following information about the user content:

*"Content created by a user is always content published by the user in [redacted]'s services. User-created content is defined in our Terms of Use as follows: "In addition to the data transferred by you from [redacted] devices, you may also save or post on some of the [redacted] services content or other material that you have created yourself, such as images, videos, text, music, comments related to the data transferred from the devices, and data on your training sessions. You can also participate in discussion forums provided by [redacted] and post links on data related to your [redacted] account on provided social*

*media channels, or link your posts there. All the content you yourself have submitted, saved, or transferred to the services provided by [redacted] is hereinafter referred to as "User Content".*

*Content created by a user is not data uploaded from the user's device or information that the user provides when creating an account. Content created by a user is data which the user himself/herself chooses to share in group discussions or [redacted]'s social media channels, for example. Typical examples of content created by a user include videos or photographs from training sessions, events or competitions. The customer owns this material but [redacted] is allowed to use and share it. This data is material which the user himself/herself has published and the data does not come from the actual [redacted] service where the customer's personal data and training data is processed.*

[redacted] *In accordance with the Terms of Use, [redacted] may reuse such data published by a user. [redacted] does not interfere with content published by a user, except when the content is forbidden or inappropriate (e.g. racist, criminal or otherwise detrimental) in accordance with the Terms of Use.*

*[redacted] will not share any user content which the user has not shared himself/herself. Neither will [redacted] share training data shared by users in the [redacted]-service, for example. Any data that is reused/re-shared was originally published by the user, which means that the user has agreed to the sharing of the data."*

### Processing of personal data for research and product development purposes

35. In addition to complaints, the Office of the Data Protection Ombudsman has, 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 processes the personal data of users on the basis of a legitimate interest for research and product development purposes. The data controller has also emphasised that the data is anonymous data. According to the controller:

    *"Only general data, such as age, gender, traineeship background, models of registered devices and applications used, will be included in the survey data. In addition to these, the research data will be connected to the training data provided by the equipment and synchronised in the [redacted] service. The data used will also be processed in such a way that individual data cannot be processed."*

36. According to the controller, it has not been possible for the user to object to the processing of personal data for that purpose.

## Written hearing of the complainants

37. According to section 34(2)(5) of the Administrative Procedure Act, the Office of the Data Protection Ombudsman has not requested the complainants to submit a response to the information provided by the controller, since the hearing of views is manifestly unnecessary.

## Written request for hearing of views and request for further clarification

38. Due to the responses received in the matter, the Office of the Data Protection Ombudsman has sent to the controller the written request for hearing of views as referred to in section 34 of the Administrative Procedure Act. In the written request for hearing of views, the controller was reserved an opportunity to be heard, and to present an opinion on the facts of the case and the preliminary assessment made by the referendary of the Office of the Data Protection Ombudsman.

## Facts of the case

39. The following facts are set out in written request for hearing of views.

General

40. When purchasing a data controller's heart rate device, the complainant does not automatically have access to [redacted] service. If the complainant wishes to use [redacted] service, it must accept the Terms of Use and Privacy Notice and give consent to the processing of personal data carried out by the controller. Consents are given by ticking the box indicating the consent. If the complainant does not wish to give consent to the processing of personal data carried out by the controller, the complainant will not have access to [redacted] service.

Consent to the processing of heart rate data

41. The controller requests explicit consent to the processing of special categories of personal data because the GDPR explicitly requires consent to be requested. Consent is also requested to improve data subjects' awareness of how the controller processes personal data.

42. [redacted] service is based on storing of data concerning the heart rate in [redacted] service. Thus, the use of [redacted] service requires a data subject to give consent to processing of data concerning the heart rate. If a customer who has purchased a heart rate device does not take [redacted] service in use but wishes to use the heart rate device in a stand-alone mode, no information on the heart rate is stored.

43. In order to take [redacted] service in use, the complainant must give consent by ticking the box that states *"I agree that [redacted] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [redacted] Privacy Notice. I can change my settings about this consent at any time."* If the complainant does not give consent to the abovementioned, the complainant is unable to register for [redacted] service.

44. The abovementioned information provided by the controller implies that the controller processes data belonging to special categories of personal data other than only data concerning the heart rate. Information on the processing of special categories of personal data is provided in Privacy Notice as follows*: "The majority of [redacted]'s services are based on data collected on our products. Some of the collected data (e.g., heart rate data) are data where we always need your consent to collect and process. This consent is requested separately in each service where data belonging to groups of personal data requiring explicit consent is processed.*[8]"

45. In addition to the obligation to request consent for heart rate data under the GDPR, the controller also requests consent in order to improve the awareness of the processing of personal data by the controller.

Consent to the transfer of personal data to third countries

46. In order to be able to register with [redacted] service, users must give their consent to the transfer of their data outside the EU/EEA. The controller has told that it transfers personal

[8] Extract provided by [redacted] from the data protection practice on its website on 17 October 2018

data under the EU-U.S. and Swiss-U.S. Privacy Shield. In countries where the Privacy Shield arrangement does not apply and the Commission has not valued an adequate level of data protection, the data has been transferred by the controller under the standard contractual clauses. The controller's grounds for transfer of personal data are also Article 49(1)(a) GDPR, i.e., explicit consent.

47. In its response, the controller has reported that it has transferred personal data outside the EU/EEA to the United States. No other third countries have been identified in the response. Thus, the Office of the Data Protection Ombudsman will only assess the transfer of data in respect of the United States.

48. The controller has informed that it requests consent to the transfer of data also because it considers that the data subjects are thus more aware of the processing of personal data carried out by the controller.

Consent to the "user content"

49. The controller requests a data subject to accept the Terms of Use which states: "*When storing, sending or transferring content to [redacted]'s services, you give [redacted] an unconditional, global, transferable and relicitable right to use, copy, present, edit, translate and share your own content created by the User. Except as regards your personal data, rights given to [redacted] cannot be revoked. [--]*. "User content" is not data from the user's device or data provided by the user's account when creating an account, but "content" created by the user refers to information that the user chooses to share, for example in group discussions or through the controller's social media channels.

50. If the complainant does not accept the Terms of Use, the complainant does not get access to [redacted] service. The controller requests the user to accept the Terms of Use in order to make users more aware of the principles and practices related to the processing of personal data.

**

51. In the written request of hearing of views, the Office of the Data Protection Ombudsman has request additional clarification. The controller was requested to provide additional information on whether it is processing other personal data concerning health belonging to special categories of personal data. In the written hearing[9], the referendary has stated that if the controller processes other personal data belonging to special categories of personal data in addition to the heart rate data, according to the referendary's preliminary assessment, the controller has not had data subject's consent to process other personal data concerning health in accordance with the GDPR. In its response to request for additional clarification, the controller has stated that it also processes the maximum oxygen uptake and the body mass index. In the written request of hearing of views, it has been noted that if the controller processes other data concerning health in addition to a heart rate data, the controller has not had a consent to the processing of such data.

[9] Under "Sanction to be proposed"

52. In the written request for hearing of views, the controller has been asked to provide clarification on the following:

    I. Does the controller process data of health other than those obtained by combining the user's age, length, weight and heart rate? Please indicate which user data the controller combines and which data belonging to special categories of personal data is being processed.

    II. The controller has told that it is processing data in order to generate value for customers. Are there other purposes for the processing of heart rate data than the abovementioned?

    III. According to the data Privacy Notice and response to additional clarifcation, data subjects have not been able to object to the processing of the data for research and product development purposes. Has the controller changed the procedure in this regard? If yes, when has the procedure changed and how has it been implemented?

    IV. How many registered persons have logged in to [redacted] service and thus gave their consent to the Terms of Use between 25 May 2018 and 18 February 2019? If the exact number cannot be given, we kindly ask you to provide an estimate of the number.

## Controller's response to written request for hearing of views

53. As explained above, the controller has been given an opportunity to express an opinion on the referendary's preliminary assessment and the facts of the case presented in written request for hearing of views.

54. The controller has been given an opportunity to provide information on requirements and information that may have an impact on the decision-making in the matter. Also, the controller has been given the opportunity to highlight circumstances referred to in Article 83(2) of the GDPR which, in the controller's view, should be taken into account when deciding and imposing any administrative fine.

55. The controller submitted a response to written request for hearing of views on 14 January 2022. In its response the controller states, inter alia, the following.

### General

56. The data controller has not been able to bring to production all the reforms it has planned that improve data protection. However, the controller says that it is investing in the development of information security and data protection. The controller states that it has made changes to prioritise a number of development projects in the area of operation, which aim, among other things, to promote identified deficiencies in the data protection practices of [redacted] service, for example.

57. [redacted]

58. The controller reports that there are millions of users in [redacted] service. In [redacted], personal data are currently equal regardless of the user's location. An effort has been made to draft [redacted]'s Privacy Notice in such a way that it would meet the requirements of many different countries. According to the controller, the data protection practice related to the service has been published in 28 language versions and a total of 49 different country and language combinations have been published.

59. The controller states that the heart rate monitor is a device that measures the frequency of the heart betting. Heart rate monitor can be a transmitter surrounded by the chest or a receiver that is attached to the wrist and resembles watch. [redacted] As a rule, the basis for measuring a heart rate is the level of activity of the user, but there are other factors contributing to it.

### Transfer of personal data

60. The data controller states that it is an international company operating in the global market, and there are different data protection provisions in its different markets. The controller states that it has explored the possibility of localising the service platform, but it has not been possible with the technology in use. In the current situation, the controller provides an equal version of its services to all areas. According to the controller, requesting country-specific consents is particularly challenging because the country information provided by the user is not reliable. In alphabetical countries, the first country is well over-represented, which suggests that the user's registration does not always complete the correct information. In the controller's view, this is a common problem in online services that do not require strong customer authentication (e.g. bank identification) that cannot even be implemented globally.

### User content

61. Between 25 May 2018 and 18 February 2019 [redacted] service has, according to the controller, included activities that rely on "user content". Users have been able to share their sports performance with followers managed by them in the [redacted] -view, where it has been possible to discuss the results. [redacted] -function has included groups, events and clubs where users have been able to discuss with other users in the same group or event and share training information for them. [redacted] -function is intended for [redacted] users who train in sports centres that use the [redacted] service. [redacted] -function also shows the sports centre's own [redacted], where the customers using [redacted] service of the sports centre have been able to share their exercises accordingly and discuss with other clients who use [redacted] service of the sports centre.

62. Sharing "user content" on platforms and discussion forums provided by the controller has been voluntary for the user. The user has also been able to choose to keep their profile private, in which case the information has not been visible to other users. Therefore, consent to the processing of the data has been necessary to allow the user to use [redacted] service of which the functions in question were an integral part. When creating their account, the user has read the Terms of Use and Privacy Notice and has given their consent to the following: *"I agree that [redacted] can collect and process my personal data in the manner described in [redacted]'s Privacy Notice. I can amend the settings related to this consent at any time."*

63. The controller has closed down [redacted]-view and [redacted] -function on 19 January 2021. [redacted]-function is still in use with regard to content other than that shared by the user, for example in order to register for lessons at sports centres.

### Controller's response to question I presented in the written request for hearing of views and request for additional clarification

64. The controller states that it does not process other data belonging to special categories of personal data in addition to the heart rate data.

65. According to the controller, it is not possible to draw any direct conclusions on a person's health other than synthesis data (raw) data or derived data collected by the controller. Some abnormality collected may be typical of specific diseases or health problems, but in the controller's view, in order to make conclusion regarding health, additional data which are not processed by the controller would be needed. The controller is of the opinion that it is generally known that significant overweight (body mass index) or low physical activity can increase the risk of multiple diseases or be associated with health problems. However, this is not automatically the case and, in the view of the controller, a person's health cannot be inferred from the body mass index or activity alone.

66. The controller states that based on user's heart rate and acceleration data the controller calculates sleeping data of which the user might notice that they have slept poorly. However, according to the controller, sleeping data cannot be used to determine the causes of poor sleep. The reason may also be related to external disruptive factors. Therefore, in order to conclude on the state of health, additional information is required of which the controller does not process.

67. The controller states that the data collected by the data controller is rather wellbeing data that the user can use when analysing their own well-being and when making changes that support it in life. It is only with the help of additional information, any medical examinations and healthcare professionals that the user can draw conclusions about their health. According to the controller, the devices manufactured by the controller are also not medical devices or meet the criteria for their approval.

68. The data collected by the controller consists of information provided by the user itself and of data collected using devices. The profile information provided by the user are gender, age, length, weight, VO2 max, maximum heart rate, resting heart rate, aerobic and anaerobic threshold, aerobic maximum speed MAS, aerobic maximum power MAP, aerobic maximum power (MAP), functional threshold efficiency FTP, target sleep time and daily activity target.

69. The user's body mass index is calculated on the basis of length and weight. In addition, the controller collects heart rate, acceleration and location data as a raw data. From this data, the controller calculates the data derived with the help of its algorithms and presents it to the user in [redacted] service. It is not possible to directly draw conclusions about the person's health from the (raw) data collected by the controller or the derived information calculated with algorithms

### Controller's response to the question II presented in the written request for hearing of views and request for additional clarification

70. In addition, according to the controller, data concerning heart rate are processed for research and product development purposes, which play a very important role in the further

development of algorithms and services. The legal basis for processing is either a legitimate interest or, in the case of separate research projects, consent of the data subject.

### Controller's response to the question III presented in the written request for hearing of views and request for additional clarification

71. According to the controller, the implementation of the objection is currently under way. [redacted] The technical planning of the objection function is scheduled for the first possible date for the first annual Quartet of 2022. Resources have been reserved for technical implementation for the next annual quartet.

### Controller's response to the question IV presented in the written request for hearing of views and request for additional clarification

72. The number of users who have approved the Terms of Use between 25 May 2018 and 18 February 2019 is 3.47 million. The controller states that they have renewed their Privacy Notice and Terms of Use on 15 May 2018, which means that during the abovementioned period most of the old users have also accepted the updated terms and conditions. New customers share of the number is 1.18 million.

## On the applicable legislation

73. The GDPR has been applied since 25 May 2018. As an EU Regulation, the GDPR is legislation directly applicable in the Member States.

74. Complaints were lodged to the Office of the Data Protection Ombudsman between 22 May 2018 and 18 February 2019. A complaint has also been lodged with the Austrian Supervisory Authority during the abovementioned period.

75. In EU law, a key principle is the principle of legal certainty. A ban on the application of retroactive legislation has been derived from this principle in several decisions of the Court of Justice of the European Union. Under that prohibition, EU law does not, as a general rule, have retroactive effect.

76. In this respect, legal practice recognises two types of retroactivity: true retroactivity and material retroactivity. "True retroactivity" means application of new legislation to sets of facts that have been fully realised during old legislation. In principle, such true retroactivity is prohibited in the legal practice of the Court of Justice of the European Union.

77. "Material retroactivity" refers to application of new legislation with effects directed at the future in a situation that arose while earlier legislation was in force, and the legally relevant activity continues under the new legislation. The Court of Justice of the European Union has accepted such material retroactivity. The Court has stated that legislation on EU law must be deemed to reach legal effects upon entry into force even when the new legislation specifies consequences of states of matters that commenced during the old legislation. When evaluating the permissibility of retroactive legislation, the Court has also paid attention to private legal subjects' need for legal protection.

78. As said, the complaints were lodged with the Office of the Data Protection Ombudsman between 22 May 2018 and 18 February 2019, i.e., both before and after application of the GDPR commenced. In the case at hand, activity subject to complaint continued after application of the GDPR had begun, and this is why the GDPR is applied to the processing of the matter.

## The applicable legislation

79. Pursuant to Article 4(1) of the 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.

80. Pursuant to Article 4(11) of the 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.

81. Pursuant to Article 4(15) of the GDPR 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. Pursuant to recital 35 of the GDPR, personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.

82. Pursuant to Article 4(22) of the GDPR 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:
(a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c) a complaint has been lodged with that supervisory authority.

83. Pursuant to Article 4(23)(b) of the GDPR 'cross-border processing' means 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.

84. Pursuant to Article 4(24) of the GDPR 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

85. Pursuant to Article 5(1)a of the GDPR personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency").

86. Pursuant to Article 6(1)(a) of the GDPR states that processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

87. Pursuant to Article 7(2) of the GDPR, if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. Under paragraph 4 of the same Article, when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

88. Pursuant to Article 9(1) of the GDPR states that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. Under paragraph 2 of the same Article, paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

89. Pursuant to Article 13(1)(c) of the GDPR states that 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 the information under Article 13 of the GDPR.

90. Pursuant to Article 49(1) of the GDPR, in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

91. Pursuant to the Article 58(2)(b) of the GDPR each supervisory authority shall have a corrective power to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR.

92. Pursuant to the Article 58(2)(d) of the GDPR each supervisory authority shall have a corrective power to order the controller or processor to bring processing operations into compliance with the provisions of the GDOR, where appropriate, in a specified manner and within a specified period.

93. Pursuant to the Article 58(2)(i) of the GDPR each supervisory authority shall have a corrective power 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.

94. Pursuant to the Article 60(1) of the GDPR the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an

endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

95. Pursuant to the Article 60(3) of the GDPR the lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

96. Pursuant to the Article 60(4) of the GDPR where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

97. Pursuant to the Article 60(5) of the GDPR where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

98. Pursuant to the Article 60(6) of the GDPR where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

## Judicial question

99. As presented above, the Data Protection Ombudsman shall review and decide on the case based on the GDPR and the Data Protection Act. The following judicial questions need to be resolved in this case:

    i. Whether the controller has been obliged to request consent to the processing of heart rate data;

    ii. Whether the controller has been obliged to inform about the processing of personal data related to [redacted] service when purchasing a heart rate device in accordance with Article 13 of the GDPR;

    iii. In addition to a heart rate data, whether the controller is processing also other data belonging to a special categories of personal data concerning health. Where the controller also processes other health data belonging to special categories of personal data, the consent requested by the controller to the processing of such data has not been specific and informed as in Article 4(11) of the GDPR;

    iv. Whether the controller has had grounds for the transfer of data to third countries; and

    v. Whether the consent collected by the controller to the processing of user content been in compliance with the GDPR?

100. If the processing of personal data by the controller has not been in compliance with the provisions of the GDPR, the Data Protection Ombudsman will assess if it should apply the corrective powers bestowed on to it under Article 58(2) of the GDPR.

101. Complaints lodged to the Office of the Data Protection Ombudsman or to the Austrian Supervisory Authority did not concern a processing operation concerning research and product development. In order to speed up the processing of these complaints, the Data Protection Ombudsman will, in this case, exclude from the decision question concerning the processing of personal data for the purposes of research and product development that has been considered *ex officio.*

## Decision and grounds of the Data Protection Ombudsman

### Decision

102. The Data Protection ombudsman takes the following view:

i. The controller has been obliged to request explicit consent to the processing of heart rate data on the basis of Article 9(2)(a) of the GDPR.

ii. The controller has not been obliged to inform about the processing of personal data in [redacted] in accordance with Article 13 of the GDPR when purchasing a heart rate device.

iii. In addition to the heart rate data, the controller also processes other data concerning the health of the data subject, when the controller is processing maximum oxygen uptake and the body mass index. The consent requested by the controller to the processing of other data concerning health has not been in compliance with the GDPR, and therefore the controller has not had a legal basis for processing other health-related data in accordance with Article 9(2) of the GDPR.

iv. At the time when the complaints were lodged, the controller had grounds to transfer data to United States.

v. 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.

### Order

103. Pursuant to Article 58(2)(d) of the GDPR, the Data Protection Ombudsman shall order the controller:

i. 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;

ii. to assess whether, in addition to heart rate data, maximum oxygen uptake and the body mass index, it processes other health data belonging to special categories of personal data when combining user-related data in [redacted] service. Where the controller processes data belonging to special categories

of personal data, the controller must ensure that it has consent under the GDPR to the processing of all data relating to health that it processes in the context of [redacted] service; and

iii. to ensure, without delay of the date of receipt of the decision that the controller has a legal basis pursuant to Article 6(1) of the GDPR to process personal data in connection with "user content".

## Reprimand

104. The Data Protection Ombudsman issues 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 has not been in line with the GDPR.

## Administrative fine

105. The controller has not had a legal basis in accordance with the requirements of the GDPR for the processing of personal data that are an integral part of the controller's core business activity, which can be considered to include the processing of data concerning health.

106. Therefore, the Data Protection Ombudsman considers that deciding whether the reprimand under Article 58(2)(b) of the GDPR constitutes a sufficient sanction for the controller's infringement regarding consent that is not in line with the GDPR should be subject to the assessment of the Collegial Body for Sanctions.

107. According to section 24 of the Data Protection Act, the administrative fine provided for in Article 83 of the GDPR is imposed by the Collegial Body for Sanctions formed jointly by the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen. To the extent that the consent concerning maximum oxygen uptake and the body mass index collected by the controller has not been in compliance with the GDPR, the matter is referred to the Collegial Body for Sanctions. The Collegial Body for Sanctions must therefore assess whether an administrative fine under Article 58(2)(i) of the GDPR is to be imposed on the controller in addition to the reprimand and orders issued by the Data Protection Ombudsman.

## Grounds

Consent to the processing of heart rate data

108. In order to register for [redacted] service, the controller has required the complainants to give consent to the following: *"I agree that [redacted] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [redacted] Privacy Notice. I can change my settings about this consent at any time*". In a complaint lodged in the Office of the Data Protection Ombudsman, the complainant has

questioned the activities of the controller, as when joining [redacted] service, the complainant had to give consent to the processing of the heart rate data.

109. According to the controller, [redacted] contains information on the maximum heart rate and resting heart rate. In the annex to the letter sent to the European Commission by the Working Party WP29[10], the Working Party considered that health data should, in a broad interpretation, concern the heart rate data measured by an application regardless of whether it is performed by medical professional or by devices and apps freely available on the commercial market and irrespective whether these devices are marketed as medical devices or not.

110. The Working Party has also considered that it is not possible to draw conclusions about a person's current or future state of health by means of an individual's registration, which includes information on the person's weight and heart rate data. The Working Party is of the opinion that in addition to the abovementioned data, at least information on the person's age or gender would be needed. In the view of the Working Party, if data on weight and heart rate were to be collected over a longer period of time and such data could be combined with data on a person's age or sex, conclusions could be drawn from the health of the data subject.

111. In [redacted] service, the controller processes information on a person's age, gender, weight, maximum and resting heart rate. On the basis of the above, the Data Protection Ombudsman considers that the heart rate data combined with other data processed by the controller reveals information on the data subject's health. Therefore, heart rate data must be regarded as data concerning health within the meaning of Article 4(15) of the GDPR, and thus the controller processes personal data belonging to special categories of personal data in accordance with Article 9(1) of the GDPR.

112. According to Article 6 of the GDPR, there must be a legal basis for processing personal data. Where the personal data processed are data concerning health, the controller must have a legal basis for processing such data in accordance with Article 9(2) of the GDPR. In the present case, since the controller processes heart rate data in order to produce an added value service, the data subject must give the explicit consent to the processing of heart rate data. Therefore, the controller has been obliged to request for consent to the processing of data concerning heart rate.

113. The complaints lodged in the Office of the Data Protection Ombudsman have not concerned whether the requested consent to the processing of heart rate data complies with the GDPR. Instead, it has been questioned whether the controller should request consent to the processing of heart rate data.

Information on the processing of personal data

[10]The Working Party on Data Protection WP29 has sent a letter to the European Commission, including annexes, clarifying the concept of health data for lifestyle and well-being applications. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

114. In complaints lodged to the Office of the Data Protection Ombudsman, the complainants considered that they had been forced to register to [redacted] service and thus to accept the processing of personal data in [redacted] service in order to use the heart rate watch.

115. The controller has reported that [redacted] service and its equipment (e.g., heart rate device) are two separate things. The controller's heart rate device and its basic functions can be used without [redacted] service. The basic functions of certain devices include measuring the heart rate, activity and exercise with default profiles, such as running, walking and cycling. Depending on the activity, basic functions enable, for example, the measurement of heart rate, consumed calories, speed, training trips, tours and duration of the exercise. However, in order to gain added value service, i.e. the utilisation of algorithms, the use of [redacted] service is required. Therefore, the customer is not tied to the use of [redacted], even though the [redacted] service is necessary for obtaining an added value service.

116. The controller states that if the device in question requires the use of [redacted] service in order to gain an added value service, information regarding this requirement can be found in its device package and in its Terms of Use. According to the controller, the customer also has right to return a device that they have purchased if they do not want to use [redacted] service. It is not within the jurisdiction of the Office of the Data Protection Ombudsman to assess whether a product or service meets the legitimate expectations of the consumer. It is within the jurisdiction of the Office of the Data Protection Ombudsman to assess whether information on the processing of personal data has been provided in a just-in-time as required by the GDPR.

117. The basic functions of the [redacted]'s heart rate watch are available without [redacted] service. Therefore, a data subject must be provided with the information before the use of the service, i.e., prior to registration in [redacted] service.

118. According to a complaint lodged in the Office of the Data Protection Ombudsman, the complainant states that they have been surprised to the fact that they had to take [redacted] service in use. However, as stated above, the heart rate device and its basic functions can be used without [redacted] service. In this context, the Data Protection Ombudsman also draws attention to the fact that, according to the controller, the data controller informs the use of [redacted] service in its device package and the customer also has right to return the device.

119. In accordance with Article 13 of the GDPR, information on the processing of personal data must be provided when personal data are collected from a data subject. The Data Protection Ombudsman considers that the controller must thus inform the data subject about the processing of personal data prior to the collection of personal data, i.e. when entering or registering into the service. When joining [redacted], customers will be able to familiarise themselves with the Terms of Use and Privacy Notice. In particular, the Data Protection Ombudsman draws attention to the fact that the basic functions of the heart rate device can also be used without [redacted] service, which is why, in the opinion of the Data Protection Ombudsman, [redacted] is not that integral part of the heart rate device that the controller's information on the processing of

personal data should not be considered sufficient in the present case. Similarly, the Data Protection Ombudsman considers that the controller's information on the processing of personal data has been transparent in accordance with Article 5(1)(a) of the GDPR.

Consent to the processing of other health data

120. As a preliminary point, the Data Protection Ombudsman draws attention to the fact that the controller's information on the processing of specific categories of personal data other than heart rate data given at the time of the registration is incompatible with the information provided by the controller in its response to the request for clarification.

121. When registering for [redacted] service, the controller informs the following: "*I agree that* [redacted] *may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the* [redacted] *Privacy Notice. I can change my settings about this consent at any time.'*

122. The Data Protection Ombudsman therefore considers that the purpose of the controller has been to seek the consent of the data subject by an act expressing consent to the processing of *other health data considered as sensitive data.*

123. However, in the response submitted to the Office of the Data Protection Ombudsman, the controller has presented that it does not process other data belonging to special categories of personal data other than data relating to heart rate.

124. The Data Protection Ombudsman will firstly assess whether, in addition to heart rate data, the controller processes other health data belonging to special categories of personal data and, secondly, whether the abovementioned practice of requesting consent for the processing of other specific categories of personal data fulfils the conditions for consent.

*Processing of health-related data in* [redacted] *service*

125. According to the response given by the controller, the data collected by the controller consists of data provided by the user themselves and of data collected with the help of devices. The profile information provided by the user is gender, age, length, weight, VO2max (maximal oxygen uptake), maximum heart rate, resting heart rate, aerobic and anaerobic threshold, aerobic maximum speed of MAS, aerobic maximum power MAP, functional threshold power FTP, target time of sleep and daily activity target.

126. The data controller has presented that it is not possible to draw any direct conclusions about a person's state of health other than heart rate, and therefore the controller, is in a position that it does not process other data concerning health. According to the controller, in order to draw conclusions about health, the controller would also need data that it does not process. The controller has considered that it is only with the help of additional information, any medical examinations and healthcare professionals that the user can draw conclusions about their health from the data collected by the data controller.

127. The controller has also considered that its devices are not medical devices or do not meet the criteria of such devices. In this context, the Data Protection Ombudsman refers to the view expressed by the Working Party on the first judicial question presented above, that the fact whether or not the device has been marketed as medical devices is irrelevant when assessing whether the data should be concerned as health data.

128. According to the Annex to the letter of the Working Party, data collected through lifestyle applications and devices should not, in general, be regarded as health-related data within the meaning of Article[11] 8 of the Personal Data Directive. The application of the GDPR has not changed the definition of health data. The Working Party's view concerns the so-called raw data, on which it is not reasonable to draw conclusions about the state of a person's health. Thus, not all information obtained from applications or devices is information about a person's health. Taking into account the wording of Article 4(15) of the GDPR "*personal data related to the health revealing his or her state of health [--]",* the Data Protection Ombudsman also considers that a single data collected by the controller does not necessarily reveal a person's state of health.

129. An example of so-called raw data given by the Working Party is the amount of steps taken by the data subject during the day, which would not be combined with other data collected about the registered user. The Working Party has also considered that the so-called raw data may, however, become health-related data when the data can be used to determine a person's state of health. Thus, the intended use of so-called raw data must be taken into account when assessing whether the data is health-related data referred in the GDPR.[12] The results of the combination of data and the purpose of the controller should also be taken into account.

130. In its guidance on the processing of health data for scientific research purposes in the context of the COVID-19 outbreak, the EDPB[13] has considered that health data can be derived from different sources, for example data may become health data by cross referencing with other data thus revealing the state of health or health risks. With regard to the concept of health data, the EDPB referred to the judgment *Bodil Lindqvist* (C-101/01[14]) of which, in paragraph 50, the Court held that the term 'data concerning health' in Article 8 of the Personal Data Directive must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the

[11] Personal Data Directive repealed by the General Data Protection Regulation
[12] The Working Party on Data Protection WP29 has sent a letter to the European Commission, including annexes, clarifying the concept of health information for lifestyle and well-being applications. Attachment to the letter: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf
[13] Guidelines 03/2020 on the processing of data concerning health for the purposes of scientific research in the context of the COVID-19 Outbreak, p. 5 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf
[14] Judgment of the Court on 6.11.2003 in Case C101-01 Göta hövrät v Bodil Lindqvist https://curia.europa.eu/juris/showPdf.jsf;jsessionid=A04867935AB30679DC72F953B32203C0?text=&docid=48382&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=2610677

health of an individual. As mentioned above, the GDPR has not changed the definition of health data.

131. It should also be noted that, under the joint guidance of the National Supervisory Authority for Welfare and Health and the Office of the Data Protection Ombudsman (30.11.2017, record no. 2810/41/2017), the Data Protection Ombudsman stated that lifestyle data is part of a broader concept of health data[15].

132. The controller has reported that it collects raw data from devices, from which it calculates data derived from its algorithms and presents to the user in [redacted]. In [redacted] service, users can see, for example, the heart rate zones during their sports activities; heartbeat (maximum and minimum) as well as calories consumed. The user will also be able to review its performance in the longer period of time. It is possible for the user to view information on their activity and sports performances by means of reports drawn up by the controller. As explained above, the controller combines the data collected on the user in order to provide the user with information on the user's activity and wellbeing as described above.

133. The Data Protection Ombudsman further highlights that not all single data should be considered data concerning health. However, if the controller will combine single data with other single data, and these combined data make it possible for the controller to draw conclusions about a person's current or future state of health, the processing of the single data may result that this data in question should be considered to be health data within the meaning of Article 4(15) of the GDPR and thus as data belonging to special categories of personal data in accordance with Article 9 of the GDPR.

134. The controller has reported that it is processing information on maximum oxygen uptake (VO2max). The controller states on its website that *OwnIndex* resulting from the [redacted] fitness test is comparable to maximum oxygen uptake ($VO2max_{)}$, which is commonly used as an indicator of aerobic fitness. According to the controller's website, the aerobic condition is related to how well the circulatory system is capable of transmitting oxygen to the body. The better aerobic condition, the stronger and more effective the heart. Good aerobic condition, among other things, reduces the risk of high blood pressure and reduces the risk of developing cardiovascular diseases or stroke.[16]

135. The controller has thus also recognized that the maximum oxygen uptake indicates the ability of the circulating system to transmit oxygen to the body and that the maximum oxygen uptake is thus linked to different diseases. The Data Protection Ombudsman considers that the information on the user's maximum oxygen uptake ($VO2max_{)}$, combined with an identifiable natural person, also indicates the person's state of health, which is why, considering the views of the Working Party and the broad interpretation of health data, the Data Protection Ombudsman considers that the maximum oxygen

[15] The guidance provided by the Office of the Data Protection Ombudsman and the National Supervisory Authority for Welfare and Health (Valvira) has concerned the transfer of samples and related information to the biobank under the Biobank Act. Data Protection Ombudsman 30.11.2017 – FINLEX ®

[16] [redacted] visited 10.5.2022 (website in Finnish)

uptake should be regarded as data concerning health within the meaning of Article 4(15) of the GDPR. In its assessment, the Data Protection Ombudsman has also noted that the controller can draw the above conclusions on the basis of the data it processes.

136. The controller has also stated in its response that the length and weight of the data subject is used to calculate the user's body mass index. The body mass index processed by the controller shall also be considered as data concerning health within the meaning of Article 4(15) of the GDPR.

137. In other respects, the Data Protection Ombudsman does not assess which other data concerning health is processed by the controller but leaves it to the controller's responsibility.

138. The Data Protection Ombudsman is of the opinion that the controller can and explicitly its purpose is to combine user's data in [redacted] in order to provide the data subject information regarding its activity with the help of algorithms. Similarly, even if the controller does not intend to directly process data concerning the health of data subjects, the Data Protection Ombudsman considers that the controller *de facto*, by combining data relating to a registered user, processes data concerning health in [redacted] service.

139. The Data Protection Ombudsman pays particular attention to the fact that the data controller has reported that the data it has collected is welfare data that users can use when analyzing their own well-being and making changes that support it in their lives.

*Consent to the processing of other health data belonging to special categories of personal data*

140. Based on the grounds presented in more detail above, the Data Protection Ombudsman has considered that, in addition to heart rate data, the controller processes at least the maximal oxygen uptake and the body mass index, i.e., also other health data belonging to special categories of personal data. According to Article 9(1) of the GDPR, the processing of such data is, in principle, prohibited. However, data concerning health may be processed, for example, on the basis of explicit consent by the data subject (Article 9(2)(a) of the GDPR).

141. The Data Protection Ombudsman notes that the purpose of the controller has been to request consent for the processing of other health related data by means of an act indicating consent, as the controller has requested consent as follows: I agree that [redacted] may collect and process my sensitive personal data, such as heart rate *and other health data considered as sensitive data* in the manner described in the controller's Privacy Notice.

142. According to Article 4(11) of the GDPR, consent must be, inter alia, specific and informed. Specific consent means consent requested for "one or more specific purposes". Specific consent therefore means that the data subject is expressly informed of the intended purposes for the use of data relating to them. In the EDPB Guidelines on Consent, the EDPB has stated that in each request for consent, the controller should *describe which data* will be

processed for each purpose[17]. For consent to be informed, data subjects must also be informed of the type or types of data collected and used[18].

143. Moreover, the processing of personal data belonging to special categories of personal data requires that consent is *explicit* in accordance with Article 9(2)(a) of the GDPR.

144. In its Privacy Notice, the controller informs that it is processing personal data for the purposes listed in the Privacy Policy. In the Privacy Notice, the controller informs, among other things, of the following:

*"When you create a user account for [redacted] services, we ask for some personal information (for example your name, email address, gender and age). We need this information in order to provide you with a personalized experience with our services. For example, we use your age info to give you a more accurate calculation of burnt calories."*

*"[redacted] is a free fitness and training app and web service that helps you track your training, activity and sleep data as well as analyze your progress. It works together with your [redacted] product and acts as your automatic training diary: all your training, activity and sleep data syncs from your product to your [redacted] account."*

145. The Data Protection Ombudsman considers that the controller *per se* informs the data subjects of the processing of their personal data for purposes such as the analysis of activity and training. However, the controller does not inform the data subjects of the types of personal data processed and of the purposes for which each type of personal data is being processed.

146. The Data Protection Ombudsman notes that the controller has, in its response to the Office of the Data Protection Ombudsman, listed data it processes. However, the same information has not been provided with the data subject at the time when the controller has requested the data subjects consent.

147. Since the controller has not provided information with the data subject on the purposes and types of data its processing, the consent requested by the controller to the processing of other health data cannot be considered as consent within the meaning of Article 4(11) of the GDPR.

148. Finally, the Data Protection Ombudsman pays attention to the fact that ICO's reply to the controller in 2018 did not concern the way in which the controller has collected consent to the processing of data belonging to special categories of personal data. In its reply, ICO stated that the controller has been able to request consent from the old users of [redacted], even though these users have already approved the processing of personal data when concluding a contract with the controller.

<u>Data transfers to third countries</u>

[17] Guidelines for consent under Regulation 2016/679, point 61, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fi.pdf
[18] Guidelines for consent under Regulation 2016/679, point 64, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fi.pdf

149. As a preliminary point, it should be noted that the controller's processing activities concerning transfer of personal data to third countries was based on the controller' procedure before 19 November 2019.

150. According to the controller, it is possible that the user's e-mail address or user ID will be transferred to a server located in the United States. The controller has reported that it has transferred data under the Privacy Shield. The Privacy Shield was repealed in the Schrems II decision of the Court of Justice of the European Union in July 2020. Thus, in February 2019 and at the time of the response given by the controller in November 2019, the controller has been able to transfer personal data to the United States on the basis of the Privacy Shield. The Data Protection Ombudsman's Office has not been informed of any transfer of data to non-EU/EEA countries other than the United States. Therefore, the transfer of data in this decision is limited to the question of the transfer of data to the United States.

151. The controller has based the transfer of data on data subjects' consent, in addition to the Privacy Shield. During the period at issue in the present case an adequate level of data protection has been guaranteed under the Privacy Shield. Therefore, there has been no need to use other legal basis as referred in Article 49 of the GDPR, for example consent.

152. As such, the GDPR does not require that in situations where personal data are transferred on the basis of explicit consent, the transfer should be occasional and non-repetitive". However, in its guidance on derogations under Article 49, the EDPB has highlighted that even those derogations which are not expressly limited to "occasional" or "not repetitive" transfers have to be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place.[19] It should be noted that, in the present case, the transfer of data by the controller to third countries was not occasional and therefore the Article 49 derogation could not have been used in the present case as a basis for the transfer.

153. In the present case, as the transfer of data by the controller was based on the Privacy Shield, the controller had an appropriate basis for transferring data to the United States. In this context, it is not necessary to assess whether the consent collected by the controller has met the conditions laid down for consent. The current data transfer practices of the controller are also not assessed in the context of the present case.

154. The Data Protection Ombudsman states that the controller must not request consent to a particular processing of personal data simply to ensure that data subjects are more aware of the processing of their personal data after having given their consent. If the processing of personal data in certain situations does not require the explicit consent of the data subject, the consent should not be collected for the sole purpose of raising awareness. However, the Data Protection Ombudsman considers that the purpose of the controller

[19] Guidelines 2/2018 on derogations of Article 49 under Regulation (EU) 2016/679 of 25.5.2018, page. 4-5 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fi.pdf

was good, as the controller has tried to raise the awareness of the data subjects.

Consent to the user content

155. According to the Terms of Use of [redacted], "by saving, submitting, or transferring content to [redacted] services, you are granting [redacted] an uncompensated, global, transferable, sub-licensable right to use, reproduce, present in public, edit, translate, and share your User Content".

156. The requirement of the [redacted] service is that a data subject accepts the Terms of Use. If a data subject does not wish to accept the above-mentioned processing operation described in the Terms of Use, a data subject does not get access to the [redacted] service.

157. First of all, it should be noted that the "accept" button should not be automatically interpreted as an act giving consent in accordance with the GDPR. In its clarifications, the controller has generally stated that the use of the [redacted] service requires consent. In the clarifications provided by the controller, the controller has not referred to any other legal basis other than consent, with the exception of processing of personal data for research and product development, in respect of which the controller has referred to a legitimate interest.[20] The Data Protection Ombudsman draws attention to the fact that, in written request for hearing of views and request for further clarification sent to the controller on 30 November 2021, the referendary of the Office of the Data Protection Ombudsman was of the opinion that consent to the processing of "user content" does not meet the conditions for consent provided for in the GDPR.[21] In its reply to the written request for hearing of views and request for further clarification on 14 January 2022, the controller has not corrected referendary's assessment by noting that it has not been controller's intension to request consent to the processing of personal data for the processing of "user content". In other words, the controller has not stated in its reply that it has not processed personal data saved, submitted or transferred by the data subject on the basis of consent.

158. In the light of the clarifications provided by the controller, the Data Protection Ombudsman considered that by ticking the "accept" button on the Terms of Use, the controller intended to request consent to the processing of personal data regarding "user content" mentioned in the Terms of Use.

159. In this decision, the Data Protection Ombudsman does not assess whether consent has been an appropriate legal basis for the processing of personal data in connection with "user content". As presented below, the Data Protection Ombudsman's assessment is limited to whether the consent chosen by the controller as the basis for processing of personal data has been in accordance with Article 7(2) and (4) of the GDPR.

160. In its clarification, the controller specified "content" as follows: "Content" is not data from the user's device or data provided by the user when creating an account, but 'content' created by the user refers to information that the

[20] See paragraph 70 of the decision
[21] Written request for hearing of views and request for further clarification, page 16

user chooses to share for example in discussions by groups provided by the controller or on the controller's social media channels. If the data subject decides to publish content by sharing, for example, a photograph on the social media channel of the controller, the data subject agrees, according to the Terms of Use, that the controller can, among other, copy, present publicly, edit and distribute content created by the user.

161. According to the controller, the [redacted] service has included functions that rely on content created by the user. Users have been able to share their results with followers managed by them, for example in the [redacted] -view and in the groups, events and clubs under the [redacted] -function. It has been possible to discuss the results in the abovementioned functions and views. Users have also been able to share training information with other users in the same group or event.

162. The Data Protection Ombudsman draws attention to the fact that the wording of the controller's information *"by saving, submitting, or transferring content to* [redacted] *services"* may have formed the impression to the complainant and possibly also for other data subjects that "content" refers to the information stored on the [redacted] service, for example during a sports performance. However, according to the controller, this is not the case. The controller does not use, copy, share publicly' the user's training data in the [redacted] service. Instead, according to the Terms of Use, the controller could process the data in the manner described in the Terms of Use when the user distributes information on the controller's platforms, such as discussion forums. The above-mentioned assumption may also have been formed since the right of the controller to process content shared by the user has been specifically described in the [redacted]'s Terms of Use and not, for example, in the Terms of Use of the platforms offered and maintained by the controller ([redacted] and [redacted]).

163. According to the controller, the [redacted] service has included functions that rely on content created by the user. However, the Data Protection Ombudsman considers that the possibility to share images or discuss in the platforms is not the core service of [redacted], even though [redacted] -function and Syöte -view have relied on information obtained from the [redacted] service. The Data Protection Ombudsman is of the opinion that the core of the [redacted] service is monitoring the user's practice and analysing progress[22]. This view is supported by the fact that the sharing of information has been based on a voluntary approach by the user, as the user can use the [redacted] service without ever sharing the information or discussing on the data controller's platforms.

164. However, as explained above, the controller has included the processing of content created by the user in the general Terms of Use, to which the data subject was required to give their consent. Therefore, the data subject has been obliged to consent to processing in which the controller has a

[22] According to the [redacted] website "[redacted] *is an exercise application and a training logbook online. When information about your traineeship, activity and sleep is available online, you can easily monitor your traineeship, analyse your progress and improve your* results. "

right to use, copy, present publicly, edit, translate and redistribute content shared by the user and obtained from the [redacted] service.

165. Consent is one of the legal basis for processing of personal data laid down in Article 6(1) of the GDPR. The consent to the processing of personal data must be, inter alia, specific and freely given. Specific consent of the data subject must be given in relation to "one or more specific" purposes. The controller must therefore make a clear separation of information related to obtaining consent for data processing activities from information about other matters.[23] According to Article 7(2) of the GDPR, if the data subject's consent is given in the context of the written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The Data Protection Ombudsman is of the opinion that the controller should not have included in its general Terms of Use the activities concerning the processing of personal data for which it intends to seek consent under the GDPR.

166. As the consent collected by the controller to the processing of content created by the user has not been requested clearly separate from other matters, the consent has not been specified and therefore does not fulfil the requirement for consent under Article 7(2) of the GDPR.

167. In this context it should be noted that the Terms Use of the service should describe the general conditions of use of the service and the processing operations necessary of that service. For this reason, the Terms of Use should not include processing operations for which consent under the GDPR should be requested.

168. The element "free" implies real choice and control for data subjects. When assessing whether the consent has been freely given, account shall be given whether consent has been attached as part of terms that cannot be negotiated. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.[24] Account should also give to the Article 7(4) of the GDPR which states that when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory

[23] Guidelines for consent under Regulation 2016/679, WP256, page 13-14 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[24] Guidelines for consent under Regulation 2016/679, WP256, page 8 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

consideration in exchange for the performance of a contract or the provision of a service.[25]

169. The controller is of the opinion that the data subject has had the right to freely choose whether or not to share images or videos in the controller's service. The Data Protection Ombudsman notes that the data subject may in fact be able to choose themselves whether or not to share information about their exercises with other users. Nevertheless, the data subject has not had a genuine free choice to consent to the processing operations described in the Terms of Use for the processing of personal data and thus this consent did not meet the condition of a freely given.

170. The Data Protection Ombudsman also draws attention to the fact that the controller has stated in its Terms of Use that it is processing personal data on a very large scale. According to the Terms of Use of the controller, the user would give the controller "an uncompensated, global, transferable, sublicensable right to use, reproduce, present in public, edit, translate, and share" content created by the user". The requirement for specific and freely given consent is also closely linked to the requirement of granularity. The consent should be granular and specific, i.e., the controller cannot request the consent of the data subject for undefined purposes or for unclear purposes. The Data Protection Ombudsman considers that the above description of the purpose of the processing is not sufficiently precise to enable the data subject to give freely given consent for specific processing activities of the controller.

171. Based on the above, the Data Protection Ombudsman considers that the consent collected by the controller to the processing of content created by the user laid down in Terms of Use has not, as a whole, met the requirements for consent referred to in Article 4(11) of the GDPR as the consent has not been, among other things, specific or freely given. As explained above, the consent has not been requested separately from other matters and it has not been possible to give consent free of choice, which is why the consent requested in this case did not meet the conditions for consent under Article 7(2) and (4) of the GDPR.

172. Data Protection Ombudsman draws attention to the fact that, as a matter of principle, content created by users may contain data concerning health. This must be taken into account when assessing the appropriate legal basis for the processing of personal data in connection with "user content", especially taken into account data subject's fundamental rights and freedoms.

173. Finally, the Data Protection Ombudsman states that, in the present decision, the Data Protection Ombudsman does not assess and it does not have competence to assess, from the point of view of the Copyright Act (404/1961), whether the data controller can process saved, submitted or transferred data without compensation and globally as described in the Terms of Use. In its decision, the Data Protection Ombudsman does not assess or otherwise take a position on the lawfulness of the processing. Thus, as regards the processing of 'user content', the Data Protection Ombudsman has limited its

[25] Guidelines for consent under Regulation 2016/679, WP256, page 11 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

assessment to whether the consent requested by the controller to the concept of ‘user content’ fulfilled the conditions for consent in a situation where the processing of ‘user content’ was based on the data subject’s consent.

The decision was made by the Data Protection Ombudsman [redacted], and it was presented by Senior Officer (referendary) [redacted].

According to section 24 of the Data Protection Act, the administrative fine is imposed by the Collegial Body for Sanctions, which has issued the following decision.

# The decision of the Collegial Body for Sanctions

## The controller

[redacted]

### Decision

174. As is apparent from the decision of the Data Protection Ombudsman, the controller did not have specific and informed consent in accordance with the Article 4(11) and 9(2)(a) of the GDPR in order to process the maximum oxygen uptake and body weight index.

175. The case does not concern minor infringements of the provisions of the GDPR, as referred to in recital 148 of the GDPR, taking into account in particular the gravity of the breach, which is why a reprimand is not a sufficient sanction.

176. The Collegial Body for Sanctions states that there are a number of circumstances in favour of not imposing an administrative fine. When assessing the requirements for imposing an administrative fine, the Collegial Body for Sanctions has, however, paid particular attention to the fact that the large-scale processing of the special categories of personal data in question is an essential part of the controller's core business, which means that an administrative fine cannot be waived. However, these other factors are of considerable importance in assessing the amount of the administrative fine.

177. In this decision, the controller has 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.

178. The controller's turnover for 2021 was [redacted]. In the present case, the administrative fine imposed to the controller shall not exceed EUR 20 000 000.

179. The Collegial Body for Sanctions jointly formed by the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen orders the controller to pay an administrative fine of EUR 122 000 (one hundred twenty-two thousand) to the State under Article 58(2)(i) and Article 83 of the GDPR. The Collegial Body for Sanctions considers the administrative fine of EUR 122 000 to be effective, proportionate and dissuasive.

## Grounds for imposing an administrative fine

### The applicable legislation

180. Pursuant to Article 83(1) of the GDPR 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.

181. Pursuant to Article 83(2) of the GDPR 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). In the present case, the Data Protection Ombudsman has ordered the controller to bring its processing operations into line with the GDPR and issued a reprimand to the controller. The administrative fine is therefore imposed in addition to Article 58(2)(b) and (d).

182. 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.

183. Pursuant to Article 83(5)(a) of the GDPR, the infringements of the provisions in this paragraph (Articles 5,6,7,9) 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.

184. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, Article 83(1)(2) and (5) shall be taken into account. When assessing the matter, consideration shall also be given to the guidelines on the application and setting of administrative fines.[26]

### Assessment of the gravity of the infringement

[26] Guidelines on the application and setting of administrative fines (wp253) https://ec.europa.eu/newsroom/article29/items/611237

185. When assessing the gravity of the infringement, Article 83(2)(a)(b) and (g) of the GDPR have been taken into account.

Nature, seriousness and duration, nature, extent or purpose of the processing

186. Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. The legislator has therefore laid down specific requirements for the processing of personal data, such as the prohibition of their processing in principle and permitted only in the circumstances permitted by Article 9. The data at issue are data concerning health within the meaning of Article 9(1) of the GDPR. Although data concerns specific categories of personal data, the Collegial Body for Sanctions considers that this data is not particularly sensitive data (cf. data concerning mental health or, for example, data on insolvency or location, which are not to be considered as a specific categories of personal data).

187. The Collegial Body for Sanctions considers that even though the processing of special categories of personal data without sufficient conditions in accordance with Article 9 does not always itself lead to the imposition of an administrative fine, but when assessing the nature and purpose of the data processing in this case, special attention must be paid to the fact that the [redacted] service, and the data concerning health that is been processed in the service, are an integral part of the core activities of the controller. These factors, taken together, reflect the gravity of the infringement and advocate the imposition of an administrative fine.

188. As a mitigating factor, the Collegial Body for Sanctions considers that the purpose of the controller is not only to develop its own product, but the purpose has also been a specifically to provide to the data subject a service to improve the well-being of the data subject. Although the controller has benefited from the processing of maximum oxygen uptake and body weight index, the processing of these data has also benefited the data subjects, as the controller has been able to develop its service using the data it has processed. Nor was the earning logic of the controller's business based solely on the processing of the data subject's data.

189. Between 22 May 2018 and 18 February 2019, complaints were lodged with the Office of the Data Protection Ombudsman. The Data Protection Ombudsman has assessed the controller's practices in the above-mentioned period. The controller has continued to violate the GDPR also after the above-mentioned date, as the controller still does not request consent as referred in the GDPR for the processing of data on maximum oxygen uptake and body weight index[27]. Based on the above, the controller's procedure under the GDPR be considered relatively long-term. However, the Collegial Body for Sanctions draws attention to the fact that the proceedings in the Office of the Data Protection Ombudsman have taken a long time. For this reason, the relatively long duration of the infringement cannot be considered to reflect the

[27] [redacted]'s website, visited on 9 September 2022

seriousness of the infringement, and this is not taken into account in the penalty assessment as a reason in favour of the administrative fine.

Number of the data subjects affected, and the level of damage suffered by them

190. As explained above, the activities of the controller have been examined with regard to complaints lodged in the Office of the Data Protection Ombudsman between 22 May 2018 and 18 February 2019. During this period, 3.47 million data subjects have approved the Terms of Use when registering for the [redacted] service. The controller has thus processed, or at least has been able to process, data on the maximum oxygen uptake and body weight index of 3.47 million users without a legal basis for the processing.

191. When assessing the impact of violations, account is taken not only of the number of data subjects but also of the fact that the processing of personal data was not just national, but the processing of personal data has also affected other data subjects located in the EU/EEA region.

192. On the one hand, the large number of data subjects reflects the seriousness of the infringement, but on the other hand according to the information available to the Office of the Data Protection Ombudsman, the data subjects have not suffered any financial damage.

The intentional or negligent character of the infringement

193. According to the guidelines issued by the Working Party, 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. It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine.[28]

194. In addition to heart rate data, the controller has also requested consent to the processing of other special categories of personal data. As indicated in the decision of the Data Protection Ombudsman, the consent requested for the processing of other data concerning health did not meet the requirements of consent laid down in the GDPR. In this respect, the Collegial Body for Sanctions draws attention to the fact that the controller's intention was to seek consent. Considering the whole, the Collegial Body for Sanctions considers that the infringement of the provisions of the GDPR cannot be considered intentional.

195. In its reply to the controller, the ICO stated that the controller has been able to change the grounds for processing, as a result of which the controller has been able to request the consent of old users[29]. Although ICO has stated

[28] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, page 11 https://ec.europa.eu/newsroom/article29/items/611237

[29] see paragraph 30 of the decision: *In light of the information you have provided, we are satisfied that [redacted]'s actions relating to the change in lawful basis for processing to rely on consent, is in compliance with your data protection obligations.*

in its communication to the controller that the controller's actions complied with the obligations arising from data protection regulation, ICO has not specifically assessed the procedure for requesting consent, which is the subject of the present decision.

196. Furthermore, the Collegial Body for Sanctions is of the view that the clarifications provided by the controller in the matter show the controller's intention to comply with the obligations of the GDPR. This is reflected, among other things, by the fact that the controller has requested consent to the processing of other health data considered as sensitive data, even if the consent has not met the requirements for consent. The Collegial Body for Sanctions also states that the complaints relate to the time when the GDPR has just started to be applied.

197. Under the one-stop-shop mechanism, the Finnish Supervisory Authority, i.e., the Data Protection Ombudsman is responsible for the supervision of the processing of personal data by the controller in question. Although another supervisory authority has assessed controller's processing of personal data, the Collegial Body for Sanctions states that controllers should also be able to rely on the assessment carried out by the supervisory authorities of other Member States.

198. However, this is not an administrative decision of an authority, but an exchange of messages between the controller and ICO. Since the correspondence does not specifically concern the issue which the Data Protection Ombudsman has assessed in this decision, and since the data processing at issue concerns the controller's core activities, the Collegial Body for Sanctions considers that the controller cannot rely solely on the communication with ICO.

199. Consequently, the Collegial Body for Sanctions considers that the circumstances described in paragraphs 195 to 198 above cannot lead to the non-imposition of an administrative fine. However, facts presented in paragraphs 194 to 197 shall be taken into account as factors that significantly reduce the amount of the administrative fine.

The categories of personal data affected by the infringement

200. As stated in the Data Protection Ombudsman's decision, the controller's conduct that violates the provisions of the GDPR has concerned the processing of maximum oxygen uptake and body weight index, i.e data concerning the data subject's health, without consent as laid down in the under GDPR.

201. The Collegial Body for Sanctions has already assessed the significance of the nature in paragraphs 176 to 177 of the decision.

## The assessment of the aggravating or mitigating factors

202. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, Article 83(2)(c) – (f), (h) – (i) and (k) of the GDPR has taken into account.

Any action taken by the controller to mitigate the damage suffered by the data subject

203. According to the guidelines issued by the Working Party when a breach occurs and the data subject has suffered damage, the responsible party (controller) should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. In accordance with the guideline, the supervisory authority may when calculating the administrative fine, take into account such responsible operations of the controller or the absence of responsible operations.[30]

204. The controller has not changed the consent collected to process maximum oxygen uptake and body weight index[31]. The Collegial Body for Sanctions does not consider this as an aggravating factor in the assessment of the fine, nor is it to be considered as a mitigating factor.

The degree of responsibility of the controller taking into account technical and organisational measures implemented by them pursuant to Article 25

205. Pursuant to Article 25 of the GDPR the GDPR requires that the controller shall take into account "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

206. As indicated in the decision of the Data Protection Ombudsman, the controller is of the opinion that the data processed by the controller cannot be used to draw conclusions on the current or future state of health of the data subject. Therefore, the controller has taken the view that it does not process data concerning health other than heart rate data. However, the controller has stated in its clarification that it processes maximum oxygen uptake and body weight index. In addition, the controller has stated on its website that the maximum oxygen absorption uptake it handles makes it possible to draw conclusions on the ability of the circulating system to transmit oxygen to the body.[32]

207. On the basis of the above, the Collegial Body for Sanctions is of the opinion that the controller has not been properly ascertained as to whether it is processing other personal data concerning health and, and if so, which health data it is processing.

Any relevant previous infringements by the controller

[30] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, 3 October 2017, page 13 https://ec.europa.eu/newsroom/article29/items/611237
[31] [redacted]'s website on 9 October 2022 [redacted].
[32] see para 134 of the decision

208. According to the guidelines issued by the Working Party the supervisory authority should assess the track record of the entity committing the infringement. Supervisory authorities should consider that the scope of the assessment here can be quite wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be "relevant" for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.[33]

209. Similar violations of the provisions of the GDPR have not been brought to the attention of the Data Protection Ombudsman. In addition, no measures referred to in Article 58(2) of the GDPR have been imposed on the controller on the same subject matter. The Collegial Body for Sanctions does not consider this as an aggravating factor nor it is to be considered as a mitigating factor.

The degree of cooperation with the supervisory authority, and the manner in which the infringement became known to the supervisory authority

210. According to the guidelines issued by the Working Party the degree of cooperation may be given "due regard" when deciding whether to impose an administrative fine and in deciding on the amount of the fine. Based on the guidelines, a note can be taken to the fact whether the entity responded in a particular manner to the supervisory authority's requests during the investigation phase in that specific case which has significantly limited the impact on individuals' rights as a result.[34]

211. Pursuant to Article 31 of the GDPR the controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks. According to the guidelines issued by the Working Party, it would not be appropriate to give additional regard to cooperation that is already required by law.

212. The actions of the controller that violate the provisions of the GDPR have come to the attention of the Office of the Data Protection Ombudsman through complaints. The controller has cooperated with the Office of the Data Protection Ombudsman. In the assessment of the administrative fine, the Collegial Body for Sanctions does not consider the above-mentioned as an aggravating factor nor it is to be considered as mitigating factor.

Any other aggravating or mitigating factor applicable to the circumstances of the case

213. The Collegial Body for Sanctions shall take into account the loss of the controller's business in recent years as a mitigating factor in the amount of the administrative fine.

[33] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, page 14 https://ec.europa.eu/newsroom/article29/items/611237
[34] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, page 14 https://ec.europa.eu/newsroom/article29/items/611237

The decision to impose an administrative fine has been taken by the members of the Collegial Body for Sanctions.

Data Protection Ombudsman [redacted] _____

Deputy Data Protection Ombudsman [redacted] _____

Deputy Data Protection Ombudsman [redacted] _____

Senior Officer [redacted] _____

*The document has been signed electronically. If necessary, the electronic signature can be verified by contacting the registry of the Office of the Data Protection Ombudsman.*

## Further information on this decision is provided by the referendary

Senior officer [redacted], tel. [redacted].

## Applicable legal provisions

The General Data Protection Regulation ((EU) 2016/679) Articles 4(1)(11)(15)(22)(23)(24), 5(1)(a), 6(1)(a), 7(2)(4), 9(1)(2a), 13(1)(c), 49, 58(2)(b)(d)(i), 60(1,-6), 83(1)(2)(5).

Data Protection Act (1050/2018) 24 §

Administrative Procedure Act (434/2003) 25 §, 34 §

## Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court by lodging an appeal in accordance with the provisions of the Administrative Judicial Procedure Act (808/2019). Appeals shall be lodged in the Administrative Court.

The appeal instructions are enclosed.

## Service of notice

The service of notice of the decision shall be effected by post against a certificate of service in accordance with section 60 of the Administrative Procedure Act (434/2003).

## Enclosures

Appeal instructions

Payment instructions of the administrative fine

## Distribution

Controller

Applicants

## Office of the Data Protection Ombudsman – contact information

**Postal address:** P.O. Box 800, 00531 Helsinki, Finland

**Tel. (switchboard):** +358 29 566 6700

**E-mail:** tietosuoja@om.fi

**Website:** www.tietosuoja.fi