noyb - European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

Autoriteit Persoonsgegevens
PO Box 93374
2509 AJ The Hague,
The Netherlands

Vienna, 31 August 2023

noyb Case-No: C-066-03

Complainant: [redacted]

represented under Article 80(1) GDPR by: *noyb* - European Center for Digital Rights, Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria

Respondent: **Fitbit International Limited**
76 Lower Baggot Street, Dublin 2, Ireland

COMPLAINT

1. REPRESENTATION

1. *noyb* – European Center for Digital Rights is a not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms with its registered office in Goldschlagstraße 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *"noyb")* (**Attachment 1**).

2. *noyb* is representing the complainant under Article 80(1) GDPR (**Attachment 2**).

2. FACTS PERTAINING TO THE CASE

3. Fitbit International Limited (hereinafter: *"Fitbit"*) offers one of the world's widely used apps for health and fitness. The Fitbit app (hereinafter: *"the app"*) has more than 50 million downloads on Google Play and can be used on its own to track basic stats or together with a tracker or smartwatch to check the user's activity, workouts, sleep, nutrition, stress, etc. In 2021, Fitbit was acquired by Google LLC, that is wholly owned by Alphabet Inc..[1]

4. Interested in these services, the complainant purchased a Fitbit Charge 3 smartwatch [redacted] (**Attachment 3**), downloaded the Fitbit app and created a Fitbit account on [redacted] to use the Fitbit app and link it to her Fitbit Charge 3 smartwatch (**Attachment 4**). In [redacted], the complainant switched to a Fitbit Charge 4 smartwatch, which she still uses today (**Attachment 5**). She also linked the Fitbit Charge 4 to her Fitbit account and to the Fitbit app to track her activities. On [redacted] the complainant subscribed to the premium version of Fitbit for an annual fee of €79.99, [redacted] (**Attachment 6**).

5. At the time the complainant created a Fitbit account on [redacted], the privacy policy that Fitbit published on 18 September 2018 applied (**Attachment 7**). This included the following text under the heading "*Our international operations and data transfers":*

> *"We operate internationally and transfer information to the United States and other countries for the purposes described in this policy.*
>
> ***We rely on multiple legal bases to lawfully transfer personal data around the world. These include your consent, the EU-US and Swiss-US Privacy Shield, and EU Commission approved model contractual clauses, which require certain privacy and security protections****. You may obtain copies of the model contractual clauses by contacting us. Fitbit, Inc. complies with the Privacy Shield principles regarding the collection, use, sharing and retention of personal information as described in our Privacy Shield certifications. Learn more about Privacy Shield here.* […]
>
> ***Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country. You agree to this risk when you create a Fitbit account and click "I agree" to data transfers, irrespective of which country you live in. For a list of the locations where we have offices, please see our company information here. If you later wish to withdraw your consent, you can delete your***

[1] https://blog.google/products/devices-services/fitbit-acquisition/

Fitbit account as described in the Your Rights To Access and Control Your Personal Data section." (emphasis added)

6. As follows from the text from Fitbit's 2019 privacy policy quoted above, in order to create an account in 2019, the complainant had to consent to the transfer of her personal data to third countries.

7. Currently applicable is the privacy policy that Fitbit published on 6 June 2023 (**Attachment 8**). In it, under the heading "*Our international Operations and Data Transfers",* almost the same text is included regarding the transfer of personal data to third countries, in particular with regard to consent and SCCs. From this text it follows:
   (i) That Fitbit continues to use "multiple" transfer mechanisms to transfer personal data to third countries, including consent and standard contractual clauses (SCCs). It is important to note, that Fitbit does not provide a definitive list as required under Article 13 (1)(f) GDPR, but only lists examples ("*These include*") of such mechanisms.
      - "*We rely on multiple legal bases to lawfully transfer personal data around the world. These include your consent and EU Commission approved model contractual clauses, which require certain privacy and security protections*." (**Attachment 8**)

   (ii) That consent to the transfer of personal data to third countries must be given when creating a Fitbit account; and
      - *"Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country. You agree to this risk when you create a Fitbit account and click 'I agree' to data transfers, irrespective of which country you live in. For a list of the locations where we have offices, please see our company information here.*" (**Attachment 8**)

   (iii) That in order to withdraw consent to the transfer of personal data to third countries, the Fibit account must be deleted.
      - "*If you later wish to withdraw your consent, you can delete your Fitbit account as described in the Your Rights To Access and Control Your Personal Data section.*" (**Attachment 8**)

8. Complainant does not have a copy of the exact text on the transfer of personal data to third countries that she agreed to at the time she created her Fitbit account. But it follows from the above versions of Fitbit's 2019 and 2023 privacy policies that the requirement of giving consent for the transfer of personal data to third countries is unchanged.

9. For illustrative purposes, **Image 1** is inserted, which shows how a Fitbit account could be created on 31 May 2023. It follows that the data subject must consent to the transfer of personal data to third countries by ticking the box with the following text: *"I agree to the transfer of my personal data to the United States and other countries with different data protection laws. Learn more*." If the data subject does not tick this box, the Fitbit account cannot be created. This is because the "*Next*" button cannot be pressed without the user agreeing to the transfer of data to third countries. The "*Learn more*" link is written in very light colours, making it practically invisible against the white background. The link leads to Fitbit's privacy policy (**Attachment 8**).

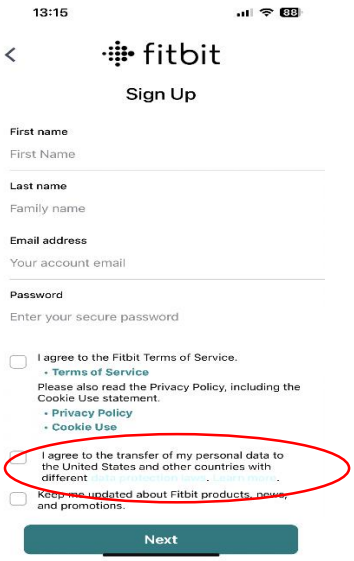

Image1.

10. Both in the request for consent to the data transfer and in Fitbit's privacy policies from both 2019 and 2023, information on the specific third countries to which Fitbit transfers its users' personal data is missing (cf. **Image 1**; **Attachment 7** and **Attachment 8**). It follows from **Image 1** that when consent is given, only transfers to the United States are explicitly mentioned. However, Fitbit's privacy policy does not inform users about which other third countries the data is sent to, nor the risks associated with these transfers. Fitbit's privacy policy includes only one link (under "*here*"), through which the data subject should be able to access a list of locations where Fitbit has offices (**Attachment 8**). However, clicking on this link leads only to a contact form and not to a list of countries where Fitbit has offices (**Attachment 9**). From the text of the policy it is obvious that Fitbit may also transfer personal data to recipients within the meaning of Article 4(9) GDPR in countries where it does not have offices. There is no list of all the third countries to which personal data of data subjects are transferred

11. In view of the foregoing, the complainant was forced to consent to the transfer of her personal data to third countries in order to complete the creation of her Fitbit account and use the Fitbit app, despite the fact that she was not fully informed of the circumstances and risks of this data transfer.

12. In privacy policy of Fitbit, it states that users must provide the following personal data *"data such as name, email address, password, date of birth, gender, height, weight, and in some cases mobile telephone number to create an account"* (**Attachment 8**). In addition, Fitbit users may also provide the following personal data *"data like logs for food, weight, sleep, water, or female health tracking; an alarm; and messages on discussion boards or to your friends on the Services"* to improve the user experience or enable certain features of the Services (**Attachment 8**). In addition to the above data, Fitbit collects data such as the number of steps they take, distance travelled, calories burned, weight, heart rate, sleep stages, active minutes and the location of the user's device. If users choose to connect to Facebook or Google, Fitbit *"may receive"* information such as name, profile picture, age, language, email address and friends list (**Attachment 8**). This personal data of complainant may therefore (potentially) be transferred to third countries.

13. According to Fitbit's current privacy policy, the data collected is processed for: a) providing and maintaining the service; b) improving, personalizing and developing the service; c) communicating with the user; and d) promoting safety and security (**Attachment 8**). The complainant's personal data may therefore (potentially) be transferred to third countries for these purposes.

14. On 15 June 2023, the complainant sent an access request to Fitbit's data protection officer ex Article 15 AVG (**Attachment 10**), to clarify how her personal data is processed by Fitbit. The complainant asked on the basis of which transfer mechanism personal data is transferred to third countries, to which third countries this personal data is transferred and what are the risks of this transfer. In addition, the complainant asked for a copy of the standard contract clauses (SCCs) in case Fitbit had used them as a transfer mechanism. The complainant also asked how she could withdraw her consent to the international transfer of her personal data.

15. Despite receiving an acknowledgement of receipt from Fitbit on its request (**Attachment 11**), the complainant has not received a response from Fitbit to this request to date.

16. In view of the above, in order to use Fitbit's services, the complainant had no choice but to consent to the international transfer of her personal data to third countries. In addition, if the complainant would like to withdraw her consent, she would have to delete her Fitbit account, as indicated in Fitbit's privacy policy, which would also prevent her from using the Fitbit app and would also terminate her subscription and therefore she would only be able to continue using her Fitbit Charge 4 to a very limited extent.

3. AUTHORITY WITH WHICH THIS COMPLAINT IS LODGED

17. [redacted]. On this basis, the complainant therefore submits this complaint under Article 77(1) AVG to the Dutch supervisory authority, being the Autoriteit Persoonsgegevens.

4. GROUNDS FOR THE COMPLAINT

4.1. Lack of transparency and information on data transfers to third countries

4.1.1. No response to the access request

18. According to Article 12(3) GDPR, the controller shall provide the data subject with the relevant information without undue delay and in any event within one month of receiving the access request. However, the complainant submitted an access request on 15 June 2023 (**Attachment 10**), but has so far not received a response other than an automated confirmation e-mail (**Attachment 11**).

19. The lack of response by the controller infringes the principle of transparency, preventing the complainant from understanding how her personal data would be processed. Consequently, it makes it impossible to exercise their rights as a data subject.

20. This amounts to a violation of Article 12 and Article 15 GDPR.

4.1.2. No transparent information on the data transfers

21. In addition, Fitbit does not specify either when asking data subjects to consent (cf. **Image 1**) or in Fitbit's privacy policy (**Attachment 8**) to which countries the complainant's data will be transferred to or which transfer mechanism is used for which transfer. Fitbit only states that personal data may be transferred "*to the United States and other countries.*" (**Attachment 8**; cf. **Image 1**).

22. Fitbit's privacy policy in addition confusingly links to a list of "*offices*" where Fitbit operates, which seems to imply that personal data will be transferred to these countries. However, the link does not lead to a list, but only to a contact page (**Attachment 8**).[2]

23. Moreover, it seems obvious that there are other recipients within the meaning of Article 4(9) GDPR (e.g. processors under Article 4(10) GDPR) in locations other than where Fitbit has its *"offices"*. Fitbit also refers to other recipients in its own privacy policy, for instance: *"Note that third-party payment processors may retain this information in accordance with their own privacy policies and terms"*[3] and *"Coaches may be provided by third parties, such as your employer or insurance company, or by our third-party coaching service providers."* (**Attachment 8**).

24. Even after the complainant asked Fitbit's data protection officer for clarification, this request was completely ignored by the company (**Attachment 10**). As a result, the complainant is still in the dark and does not know to which countries her personal data is being transferred, the risks posed by these transfers and on which Chapter V GDPR mechanism each of these transfers is based.

25. Therefore, Fitbit violated Articles 5(1)(a), 12, 13(1)(f), 44 and 49(1)(a) GDPR.

4.2. Violation of Chapter V GDPR: lack of legal basis for transferring personal data to third countries

4.2.1. Fitbit cannot rely on multiple legal bases for third-country transfers

26. Article 49 GDPR provides that "**in the absence** *of an adequacy decision (…) or of appropriate safeguards pursuant to Article 46*" (such as SCCs), "*a transfer or a set of transfers of personal data to a third country*" may be based on one of the derogations for specific situations (such as explicit consent).

27. "*In the absence of*" means that when Fitbit, as a controller, bases the transfer of personal data to a third country on SCCs, it cannot simultaneously use explicit consent as a mechanism for the same transfer.[4]

---

[2] Fitbit Privacy Policy 6 June 2023: "*For a list of the locations where we have offices, please see our company information here*". The link leads to a "*Contact Us*" page: https://www.fitbit.com/global/us/about-us.

[4] See: EDPB Guidelines 02/2018, p. 3-4; Kuner, Bygrave, Docksey, *The EU General Data Protection Regulation (GDPR), A commentary,* Oxford: Oxford University Press 2020, p. 846: "*As provided in Article 49(1) GDPR, the derogations under*

28. As further clarified by the EDPB in its Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679, *"data exporters should first endeavour possibilities to frame the transfer with one of the mechanisms included in Articles 45 and 46 GDPR, and only in their absence use the derogations provided in Article 49 (1*)."[5]

29. Contrary to the wording of the GDPR and the EDPB Guidelines, Fitbit argues that it relies *"on multiple legal bases to lawfully transfer personal data around the world",* (**Attachment 8**), including **both** explicit consent (Article 49(1)(a) GDPR) **and** SCCs (Article 46(2)(c) GDPR).

30. Therefore, Fitbit violated the provisions of Chapter V GDPR, in particular Articles 44 and 49(1) GDPR.

4.2.2. Using both SSC and consent as legal bases for third-country transfer is unfair

31. In addition to not being transparent, the information provided by Fitbit about transfers of personal data to third countries is unfair.

32. When users are creating a Fitbit account, they are required to consent to the transfer of their data to the US and other countries. This creates the false impression that they have a certain level of control over these transfers. However, Fitbit's privacy policy states that Fitbit relies on multiple legal bases, including SCCs. This means that users have no control over the transfers of their data to third countries. Consequently, information provided by Fitbit is misleading and generates expectations on users that do not correspond to how it actually transfers personal data to third countries.[6]

33. Moreover, it is also unclear what would happen if complainant could withdraw her consent for the data transfers. It is uncertain if the data transfers would stop or if Fitbit would continue to transfer complainant's data by just 'switching' to SCC's. According to the EDPB: "*It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals. In other words, the controller cannot swap from consent to other lawful bases*."[7] Therefore: "[…] *controllers must have decided in advance of collection what the applicable lawful basis is*." This is something Fitbit clearly did not do.

34. Moreover, by the wording that is chosen by Fitbit in their privacy policy, Fitbit also seems to be trying to transfer the existing risks related to data transfers to the complainant, since the complainant has to consent to and to agree with all the risks related to data transfers to third countries: "*Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country.*

Article 49 are designed to be used in situations when no adequacy decision has been issued with regard to the third country of data transfer, and appropriate safeguards cannot be used. That is, Chapter V of the GDPR sets up a three-tiered structure for legal bases for data transfers, with adequacy decisions at the top, appropriate safeguards in the middle, and derogations at the bottom. This means that if an adequacy decision has been issued then it should be relied on; if not, then appropriate safeguards should be used; and only if neither of these legal bases is available should the derogations be relied on."

[5] EDPB Guidelines 02/2018, p. 4.

[6] Cf. EDPB Guidelines 03/2022, para. 9; Recital 39, 42 and 60 GDPR; Article 13(2) GDPR.

[7] EDPB Guidelines 05/2020, para. 122-123.

***You agree to this risk when you create a Fitbit account and click "I agree" to data transfers**, irrespective of which country you live in*." (**Attachment 8**) (emphasis added). According to the EDPB the (intended) transfer of such risks violates the principle of fairness too.[8]

35. As already emphasized, the information provided by Fitbit when consent to the data transfers is sought and the information provided by Fitbit in its privacy policy on data transfers to third countries is not transparent and therefore also violates the principle of fairness (cf. **Image 1** and **Attachment 8**). This prevents the complainant from understanding the data transfers and their consequences and from exercising her rights in this regard.[9]

36. For the above reasons, Fitbit violates the principle of fairness provided by Article 5(1)(a) GDPR.

4.2.3. Consent is not an appropriate legal basis for systematic transfers of personal data to third countries

37. It follows from the EDPB guidelines that the term ***"occasional"*** in recital 111 GDPR and the term ***"not repetitive"*** in Article 49(1), second paragraph GDPR mean that the "*derogations for specific situations*" of Article 49 GDPR) cannot be used as a legal basis for the systematic transfer of personal data to third countries that do not provide an adequate level of protection, such as the United States.[10]

38. In this sense, derogations such as *"explicit consent" "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"* [11] (emphasis added).

39. In the present case, the transfers of the complainant's personal data to third countries cannot be considered occasional, as they clearly occur on a regular and systematic basis.

40. In addition, the Autoriteit Persoonsgegevens states on its own website: "*For transfers to the US, however, you cannot easily invoke such an exception [from Article 49 GDPR]. You have to weigh up the situation on a case-by-case basis*."[12]

41. Therefore, consent cannot be an appropriate legal basis for the transfer of the complainant's personal data to third countries, in violation of Article 49 GDPR.

4.2.4. Consent is invalid

42. Even if consent could be used by Fitbit as a legal basis for mass, repetitive and systematic transfers of personal data to third countries, such consent is invalid because it does not meet

[8] Cf. EDPB Guidelines 04/2019, para. 70.
[9] Cf. EDPB Guidelines 03/2022, para. 73.
[10] EDPB Guidelines 02/2018, p. 4.
[11] EDPB Guidelines 02/2018, p. 4.
[12] https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-naar-de-vs, last viewed on 08-08-23.

the general requirements of Article 4(11) and Article 7 GDPR, nor the specific consent requirements of Article 49(1)(a) GDPR.[13]

4.2.4.1. Consent is not informed

43. According to EDPB Guidance 05/2020 on consent under Regulation 2016/679, *"providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing".*[14]

44. Moreover, with regard to international data transfers, Article 49(1)(a) GDPR explicitly requires that the data subject, ***"after having been informed***" of the potential risks that such transfers may entail, gives his or her explicit consent.

45. In its Guidelines 02/2018, the EDPB further clarifies that Article 49(1)(a) GDPR also requires that data subjects be informed of the **specific risks** arising from these transfers and about the absence of appropriate safeguards.[15] According to the EDPB, " *The provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer and therefore* ***if it is not supplied, the derogation will not apply.***"[16] (emphasis added)

46. Moreover, to be complete, this information required by Article 49(1)(a) GDPR must specify the following:
    - all recipients of data or categories of recipients;
    - all countries to which personal data is transferred;
    - that consent is the legal basis for the transfer; and
    - that the third country to which the data is transferred does not provide an adequate level of data protection based on a European Commission decision.[17]

47. As already set out in section 2 of this complaint, such information was never provided to the complainant, neither when consent to the transfer was requested, nor in Fitbit's privacy policy, nor after the submission of the access request (**Image 1**; **Attachment 8** and **Attachment 10**). In particular, the list of countries to which her personal data is being transferred was never provided to her, and the specific risks (at least those related to transfers to the United States) were nowhere specified.

48. About these risks, Fitbit merely states that "*the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country. You agree to this risk when you create a Fitbit account and click 'I agree' to data transfers, irrespective of which country you live in.*" (**Attachment 8**).

[13] EDPB Guidelines 02/2018, p. 7.
[14] EDPB Guidelines 05/2020, p. 16.
[15] EDPB Guidelines 02/2018, p.7.
[16] EDPB Guidelines 02/2018, p. 9.
[17] EDPB Guidelines 02/2018, p. 9.

49. For the foregoing reasons, the consent obtained from the complainant was not informed as required by Articles 4(11), 7(1) and 49(1)(a) GDPR.

4.2.4.2. Consent is not specific

50. According to the EDPB, *"Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer at the time of the collection of the data, e.g. if the occurrence and specific circumstances of a transfer are not known at the time consent is requested, the impact on the data subject cannot be assessed*".[18]

51. As developed in Section 2, Fitbit never provided information on the specific circumstances of the transfer (cf. **Image 1** and **Attachment 8**). For instance, Fitbit never provided the list of countries to which the Complainant's personal data is transferred, nor the purposes for which such personal data is transferred, nor did Fitbit inform the complainant about the specific risks.

52. For these reasons, consent cannot be considered specific as required by Articles 4(11), 7(2) and 49(1)(a) GDPR.

4.2.4.3. Consent is not freely given

53. The "core" element of consent is the fact that it must be freely given, as clarified in Article 4(11) GDPR and further specified in Article 7(4) GDPR.

54. According to the latter provision, to assess 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"* (emphasis added).

55. As further clarified in recital 43 GDPR: *"Consent is presumed not to be freely given (…) if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."*

56. In this sense, consent can only be a lawful ground for processing if data subjects are offered a genuine and realistic choice to accept the terms of a service or to decline it **without detriment** (recital 42 GDPR, *in fine*).

57. From EDPB guidelines, it follows that *"if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment."*[19]

58. The Court of Justice already confirmed that consent could not be considered as free if the terms of that contract are capable of misleading the data subject as to the possibility of

[18] EDPB Guidelines 02/2018, p. 8.

[19] EDPB Guidelines 05/2020, p. 8.

concluding the contract in question even if he or she refuses to consent to the processing of his or her data.[20]

59. In the present case, the complainant was forced to consent to the transfer of her data to third countries and now is forced to delete her Fitbit account and no longer use the app if she wishes to withdraw her consent to the data transfer (cf. **Image 1** and **Attachment 8**). In short, once consent is withdrawn, the complainant can only use the features of her Fitbit Charge 4 smartwatch to a very limited extent.

60. This contradicts the EDPB guidelines, according to which the *"controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent."*[21] According to the EDPB, "detriment" includes the fact that "*the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way)."*[22]

61. For these reasons, consent cannot be regarded as freely given as required by Articles 4(11), 7(4) and 49(1)(a) GDPR.

4.2.4.4. Consent cannot be easily withdrawn

62. Article 7(3) GDPR establishes that it shall be as easy to withdraw as to give consent. According to the EDPB, *"the requirement of an easy withdrawal is described as a necessary aspect of valid consent.*[23] However, in the case at stake, this requirement is not met.

63. It follows from Fitbit's privacy policy that if the complainant wants to withdraw her consent to the transfer of her data to third countries she has to delete her account: "[...] *If you later wish to withdraw your consent, you can delete your Fitbit account as described in the Your Rights To Access and Control Your Personal Data section*." (**Attachment 8**). However, the "Your Rights To Access *and Control Your Personal Data* section" does not include any information about withdrawing consent to international data transfers, users can only find information on how to delete their Fitbit accounts under the heading "*Editing and Deleting Data"* therein.

64. Fitbit's privacy policy does include information on how to users can withdraw consent in a more general sense, referring to the possibility of doing so via the *"account settings*" (**Attachment 8**).[24] It happens that neither the withdrawal of consent in a general sense (as referred to in Article 6(1)(a) GDPR) nor the withdrawal of consent for transfers of personal data to third countries (as referred to in Article 49(1)(a) GDPR) are not possible via the account settings in the app (**Attachment 12**).

---

[20] CJEU 11 November 2020, C-61/19 (*Orange Romania*), para 52.

[21] EDPB Guidelines 05/2020, para 46.

[22] EDPB Guidelines 05/2020, para 49.

[23] EDPB Guidelines 05/2020, para 116.

[24] E.g. Fitbit Privacy Policy 6 June 2023: "*You can use your account settings and tools to withdraw your consent at any time, including by stopping use of a feature, removing our access to a third-party service, unpairing your device, or deleting your data or your account.*"

65. However, according to the EDPB, if consent is obtained by electronic means, data subjects must be able to withdraw that consent equally as easily. Moreover, the data subject must not suffer any detriment. *"This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels."*[25]

66. It follows that, in the present case, consent does not meet the requirements of Articles 4(11), 7(3) and 49(1)(a) GDPR.

4.2.4.5. Conclusion: consent is invalid

67. For the reasons set out above, consent cannot be considered valid within the meaning of Articles 4(11), 7, 6(1)(a), and 49(1)(a) GDPR.

4.2.5. SCCs are not an adequate legal basis for transferring personal data to the US

68. Despite not specifying the complete list of countries to which it transfers its users' personal data, Fitbit confirms that it transfers such data to the United States. (**Image 1** and **Attachment 8**).

69. For transfers of personal data to the United States, Fitbit also appears to use SCCs, according to the Fitbit privacy policy (**Attachment 8**).[26] This information was not confirmed by Fitbit, although the complainant explicitly asked Fitbit's data protection officer in her request for inspection (**Attachment 10**).

70. Even if the complainant was never granted access to Fitbit's SCCs, the fact is that the transfer of personal data to the United States based on SCCs requires additional safeguards to ensure a level of protection equivalent to that of the EU. The Personal Data Authority also states on its own website: "*When transferring to the US, you must take additional measures in this regard*."[27]

71. Indeed, it follows from the CJEU's judgment in C-311/18 (*Schrems II*) that *"standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country"*.[28]

72. The CJEU goes further to state that *"in so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of*

[25] EDPB Guidelines 05/2020, para 114.

[26] Fitbit Privacy Policy 6 June 2023 under "*Our International Operations and Data Transfers*": "[...] *We rely on multiple legal bases to lawfully transfer personal data around the world. These include your consent and* ***EU Commission approved model contractual clauses***. [...]" (emphasis added).

[27] https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-naar-de-vs, last viewed on 08-08-23.

[28] CJEU 16 July 2020, C-311/18 (*Schrems II)*, para 133.

supplementary measures by the controller in order to ensure compliance with that level of protection."[29]

73. After the CJEU ruling, the EDPB issued the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. In these recommendations, it clarifies that *"the situation in the third country to which you are transferring data may still require that you supplement these transfer tools and the safeguards they contain with additional measures ('supplementary measures') to ensure an essentially equivalent level of protection."*[30]

74. More recently, when deciding the dispute submitted by the Irish supervisory authority on data transfers by Meta Platforms Ireland Limited for its Facebook service, the EDPB referred to these guidelines and stated that *"when assessing third countries and identifying appropriate supplementary measures, controllers should assess if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools that they are relying on."*[31]

75. In the case of the United States, where domestic law provides for the possibility of public authorities to access personal data transferred from abroad as recognised by the CJEU, SCCs are clearly not enough to ensure an equivalent level of data protection without any supplementary measures. [32]

76. That is precisely the reason why the EDPB considered that Meta seems *"to simply ignore the ruling of the CJEU", "seeking to promote a lower standard for the objective of SCCs and supplemental measures than is permitted by the Judgment and the GDPR."*[33] More specifically, the EDPB recognized that Meta *"does not have in place any supplemental measures which would compensate for the inadequate protection provided by US law."*[34] Similarly, Fitbit does not mention such supplementary measures.

77. Based on the above, Fitbit violates Articles 44 and 46(2)(c) GDPR.

4.2.6. Conclusion: no valid legal ground for third-country transfers

78. Due to the lack of a valid legal ground for the transfers of personal data to third countries - as Fitbit does not meet either the requirements of Article 49(1)(a) GDPR or the requirements of Article 46(2)(c) GDPR - Fitbit violated he provisions of Chapter V GDPR.

5. REQUEST

79. In order to comply with Articles 12, 13 and 15 GDPR, the complainant requests the competent supervisory authority **to order Fitbit to provide complete information** on the international transfers of her personal data, considering that Fitbit has not responded to her access request.

[29] CJEU 16 July 2020, C-311/18 (*Schrems II)*, para 133.
[30] EDPB Recommendations 01/2020, para 23.
[31] EDPB Binding Decision 1/2023, p. 35.
[32] CJEU 16 July 2020, C-311/18 (*Schrems II)*, para. 180 et seq.
[33] EDPB Binding Decision 1/2023, p. 35.
[34] EDPB Binding Decision 1/2023, p. 35.

The information provided by Fitbit should include at least the information required by the GDPR, including but not limited to:

a) The identity of all data recipients;
b) All countries to which personal data is transferred;
c) Which is the legal ground for of each of these transfers;
d) If the legal ground is SCCs, to provide a copy of these clauses;
e) The purpose of these transfers;
f) What are the specific risks associated with these transfers;
g) The existence or absence of supplementary safeguards;
h) If supplementary safeguards have been put in place, what are these supplementary safeguards.

80. The Complainant also requests the competent supervisory authority to state:

a) That Fitbit can only rely on one legal ground for each transfer of personal data to third countries;
b) That SCCs are not an appropriate legal ground for Fitbit to transfer her personal data to the United States;
c) That consent is not an appropriate legal ground for Fitbit to transfer her personal data to third countries;
d) That the consent given for transfer of her personal data to third countries is invalid; and therefore
e) That the transfers of her personal data to third countries by Fitbit is unlawful.

81. The complainant also requests the competent supervisory authority **to order Fitbit**:

a) To bring its processing operations into compliance with Chapter V of the GDPR, by ceasing the unlawful processing, including storage, outside the EU/EEA of personal data of complainant transferred in violation of the GDPR;
b) To allow the complainant to withdraw her consent for international transfers without detriment and, in particular, without having to delete her account.

82. Finally, the complainant requests that the competent supervisory authority impose a fine on Fitbit for the various violations mentioned in this complaint. In accordance with Article 83 GDPR, this fine should be based on Alphabet Inc.'s annual turnover, as Fitbit is owned by Google LLC, that is wholly owned by Alphabet Inc.

6. CONTACT

83. Communication between the *noyb* and the authority in these proceedings should be by e-mail at [redacted]