FORBRUKERRÅDET

To
The Norwegian Data Protection Authority
post@datatilsynet.no

The Consumer Ombudsman
post@forbrukerombudet.no

Oslo 3.11.2016

Complaint regarding terms of use and privacy policies for the Fitbit Charge HR, Garmin Vivosmart HR, Jawbone UP3 and Mio Fuse activity wristbands

The Norwegian Consumer Council hereby lodges a formal complaint regarding four activity wristbands for sale through the Norwegian market. The wristbands in questions are Fitbit Charge HR, Mio Fuse, Garmin Vivosmart HR and Jawbone UP3.

Point-by-point summary of the complaint:

- The user agreements give narrow and vague definitions of what is considered personal data
- Users are not given advance notice of changes to the terms of use
- Users are not told which third parties the data is shared with
- Procedures for deleting user data are inadequately explained
- Users are not notified if they are at risk of being blocked from the service
- User data portability is not possible

Background
So-called wearables are items worn on or attached to the body. With the help of sensors and a mobile application, they track and store information about the user's heart rate, training activity, calorie intake etc. Activity wristbands (also known as fitness or activity trackers) are a popular category of wearables and are, simply put, digital watches equipped with "smart" technology such as a heart rate monitor, pedometer, calorie counter and barometer. By wearing an activity wristband, users can access detailed information and statistics about their training and other physical activity, depending on which functions are offered in the accompanying app. If there is a social element to the app[1], you can also compare your own activity with that of other users.

The Norwegian Consumer Council has looked at the activity wristbands Fitbit Charge HR, Mio Fuse, Garmin Vivosmart HR and Jawbone UP3 as part of a larger project dealing with the internet of things. All four wristbands are ubiquitous in the Norwegian market, and the number of global downloads from Google Play indicates this. Fitbit's official app has been downloaded between 10 and 50 million times on Google Play, Garmin Connect between 5 and 10 million times, Mio Go between 100,000 and

[1] Can be linked to Facebook, for instance.

500,000 times, and Jawbone UP between 1 and 5 million times.[2] The number of downloads from Apple's App Store are not publically available, but a considerable portion of additional downloads from the App Store can be assumed.

The Norwegian Consumer Council has looked at the terms of use and privacy policies (hereafter collectively referred to as terms of use) for the four activity wristbands. Our examination looked at certain aspects of the terms of use that have consequences for consumers, and we have applied European legislation as a basis for comparison and evaluation. The study was carried out by downloading the apps from Google Play. All of the four apps have a link to their terms of use in the app store, and the terms of use and privacy policies were read on the web pages containing these for each app.

Legal issues – legal person

From what we have been able to find out, the following companies supply the apps for the respective activity wristbands:

Fitbit Charge HR:

At www.fitbit.com the company's name is stated as Fitbit, Inc. and its address as Fitbit, Inc., 405 Howard Street, San Francisco, CA 94105.

As far as we are aware, the company is not registered with Privacy Shield[3] as of October 26th. According to their own Privacy Policy, Fitbit follows Privacy Shield terms, and we therefore assume that they are in the certification process.

Fitbit has registered several entities in Europe, see the European Business Register.[4] On its website, www.fitbit.com, the company gives 76 Lower Baggot Street, Dublin 2, Ireland as its sole point of contact in Europe. According to an Irish newspaper story, two entities have been established in the Republic of Ireland: one limited company (Fitbit International Limited – company no. 546599) and one unlimited company (Fitbit International Holdings – company. no 546598). Both companies can be found by performing a search of the European Business Register. To our understanding, the company's activities in Ireland were established and are owned by Fitbit, Inc. in the U.S., and this is the head office[5] for Fitbit's European operations.

Garmin Vivosmart HR:

On the basis of information published at www.garmin.com, we assume Garmin International, Inc., 1200 East 151st Street, Olathe, Kansas 66062, USA to be the correct legal person. According to Section 2A. of the Privacy Statement, this company is responsible for "managing jointly used Personal Information".

As far as we are aware, the company is not registered with Privacy Shield as of October 26th.

A search of the European Business Register shows that Garmin has established multiple entities in Europe. They include one company by the name Garmin (Europe) Limited (company no. 02724437),

[2] Figures obtained from Google Play September 2016.
[3] https://www.privacyshield.gov/list
[4] https://w2.brreg.no/ebr/
[5] http://www.independent.ie/breaking-news/irish-news/fitbit-to-create-50-jobs-at-new-european-hq-in-dublin-35009773.html

Liberty House, Bulls Copse Road, Hounsdown Business Park, Southampton, SO40 9LR, UK. Both of these companies are subsidiaries of Garmin Ltd., which is based in Switzerland.

In Norway, the company is registered as Garmin Nordic Norway AS, Dillingtoppen 15, 1570 Dilling, with the following organization registration number 987 199 423. As we understand it, products bought in Norwegian online Garmin store, https://buy.garmin.com/nb-NO/NO/view-cart.ep, is delivered by the mentioned in the terms of the website; http://www.garmin.com/nb-NO/legal/shopterms.

Jawbone UP3:
According to the terms of use on Jawbone's website, the app supplier is AliphCom, Inc., 99 Rhode Island Street, 3rd Floor, San Francisco, CA 94103. We have not identified any European links or business registrations for this company, except for the statement at www.jawbone.com/about that the company is "*Headquartered in San Francisco with offices globally*…".

The company is not registered with Privacy Shield from what we can tell.

Mio Fuse:
Physical Enterprises Inc., 2930 Arbutus Street, Suite 302, Vancouver, BC, V6J 3Y9, Canada is the company behind the Mio Fuse activity wristband. We have found no European links or business registrations for the company.

The company is not registered with Privacy Shield as far as we are aware.

Governing law and jurisdiction – the Norwegian Personal Data Act
The Norwegian Personal Data Act applies to "controllers who are established in Norway." Every company must be deemed to be a controller in the sense expressed in the Personal Data Act, and the question is whether this establishment criterion has been met by any of the above-mentioned companies. From what we can tell, the question is most relevant regarding Fitbit and Garmin, which are both registered in Europe. We ask the Data Protection Authority to consider whether these companies' operations are of a nature that could invoke the law on the processing of personal data.

The Personal Data Act may also be applied to controllers established outside of the EEA if the controller "makes use of equipment in Norway". The exact scope of the equipment criterion has not been definitively settled in case law, administrative practice by the Data Protection Authority, or decisions by the Privacy Appeals Board. A broad understanding of the term must be applied, and it extends to all equipment, both electronic and non-electronic, that can be used to process personal data.[6] As well as being equipment in the physical sense, the equipment must also be used for the collection of data, and the controller must be intending to process personal data. The controller does not have to own or have full control over the equipment.

The Article 29 Working Party has made a statement on the issue. The Working Party is made up of members from the national data protection authorities, the European Data Protection Supervisor and the European Commission, and its interpretation of the Data Protection Directive should therefore be given some weight. Concerning the downloading of apps to devices, the Working Party writes the following about the equipment criterion in its Opinion 02/2013: "Since the device is

[6] White Paper "Ot.prp. nr. 92" (1998–1999), page 107

instrumental in the processing of personal data from and about the user, this criterion is usually fulfilled." A Working Paper from 2002[7] considers the use of cookies and JavaScript to fulfil the equipment criterion.

The Norwegian Consumer Council believes that there are strong arguments in favour of deeming the equipment criterion to be fulfilled for apps associated with activity wristbands.

The activity wristbands are being sold by the largest retailers in Norway, including sports and electronics chains both in physical outlets and online. Activity wristbands will not work / cannot be used without downloading an associated app to a secondary device. Some of the apps have published Norwegian versions of their terms of use and website.[8] The user must also register / create an account in the app and then synchronise the activity wristband with the app. Once the user has registered and synchronised the activity wristband, data can be recorded by the wristband and automatically transferred to a mobile app via Bluetooth. The app sends this data to a server[9] for processing/analysis, and the data is then returned to the app. It is also common for users to receive general and/or individual feedback on activity targets, for instance.

The activity wristband and app are complementary, i.e. a user cannot make full use of the wristband without downloading the app and vice versa. The companies manufacture, market and sell both the activity wristbands and associated apps. An activity wristband together with an associated app on a secondary device give the companies access to, and the opportunity to process personal data on, the user.[10] One could ask whether a complementary instance such as this between wristband and app is sufficient for meeting the equipment criterion.

It would be unfortunate if the scope for applying the equipment criterion is restricted by undermining the very reasons for giving everyone a high degree of privacy.[11] This is something European consumers could be risking if the equipment criterion is not applied in cases such as this one, where a company with direct influence and control over the entire "value chain" is able to bypass European privacy rules.

This is also a case of processing health information, and sensitive personal data about individual users requires strong protection – another argument for applying the equipment criterion.

Governing law and jurisdiction – the Norwegian Marketing Control Act

The Consumer Ombudsman is charged with overseeing compliance with the Marketing Control Act, and in previous cases the Ombudsman has stated that its regulatory powers extend to cases similar to this one.[12] One common factor in this complaint is that all the companies involved are targeting their operations at Norway, in that their activity wristbands are being sold in Norway and that the

[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf

[8] During our review Garmin was found to be the only provider offering Norwegian versions of its terms of use and website.

[9] Controlled by the service provider.

[10] Mio is the only app with an opt-in for the processing of personal data.

[11] See Directive 95/46/EC, Article 1 cf. preliminary item 20.

[12] Cf. http://fbrno.climg.no/wp-content/uploads/2016/03/20160301-Klage-på-urimelige-avtalevilkår-Tinder.pdf, and https://forbrukerombudet.no/content/2016/07/Brukervilkår-til-Tinder-Inc.-–-mfl.-§-22-L340135.pdf.

service providers have made the apps associated with each wristband available to Norwegian consumers from Google Play and Apple's App Store.

Additional information about the issues that the regulators are asked to consider is outlined in the following, and elaborated upon in Annex 2 and 3.

Definition of personal data, acceptance of terms, and consent to data processing
First we should like to express our general concern that these services are ambiguous in their explanation and definition of personal data in the terms of use, and that little is done to seek consent for the processing of personal data, cf. Section 8 of the Personal Data Act. Our study has found that two of the four services (Mio and Fitbit) defines personal data in line with European and Norwegian rules, see appendix 2 page 11. We note that Fitbit are in the process of registering with Privacy Shield, and we have been informed that they will comply with European legislation. Privacy Shield terms are not directly linked to from the Fitbit frontpage *www.fitbit.com*. However, we have observed that Privacy Shield terms are linked to from the Fitbit Privacy Policy dated August 10th 2014. [13] Apparently Fitbit have added these changes without notice, and without updating the date on the top of the document.

In their privacy policy, Mio state that:

"Personal information is any information that identifies you personally, either alone or in combination with other information available to us." (Mio PP[14])

Garmin's terms describe personal data thus:

"'Personal Information'" is information that identifies a particular individual. […] If you reside in a country outside the United States, please note that the data protection and privacy laws of the United States may not be as comprehensive as the laws in your country."

Jawbone describes which information it collects, although its terms of use are unclear about whether this constitutes personal data.

Previous studies[15] have found that just four location points are sufficient to identify a person. Location thus constitutes personal data in many cases. We have noted that the activity wristbands provide little information about how they define and process location data.
There is cause for concern when, during their review of mobile applications in March 2016, and in their latest investigation into activity wristbands, the Norwegian Consumer Council has found the providers to be quite ambiguous about how they define and process personal data. We have observed that they use narrow and often vague descriptions of what they consider personal data, in the form of definitions of personal data that deviate from European rules. Defining information as personal data would strengthen consumer protection, and those processing the information are

[13] https://www.fitbit.com/no/legal/privacyshield (as of October 26th 2016)
[14] Second paragraph under the header "What types of personal information do we gather?"
[15] http://phys.org/news/2013-03-easy-identity-cell.html

given greater responsibility than if the information is not treated as personal data. The Norwegian Consumer Council therefore urges the regulators to look at the matter in order to ensure that consumer privacy is maintained.

The Norwegian Consumer Council believes that a number of questions can be raised about user acceptance of terms of use and privacy policies (hereafter referred to as terms of use), and about seeking consent for the processing of data. Our study found that the terms of use are generally easily accessible to users who download an app and create a user account. However, easy access does not mean that the contents of the terms of use are clear and easy to comprehend, bearing in mind that the agreements are entered into on (small) mobile devices, are overwhelming in length, and often contain complex language. We have found that the terms of use for three of the four activity wristbands are in English, and that the average word count for the four wristbands is just over 6,300 words. We question whether the way in which the terms of use are presented to the user could be in breach of the Marketing Control Act and Personal Data Act, and ask for this to be investigated.

Notification of changes to the terms of use

None of the four services commits themselves to notifying users *before* making changes to their terms of use, cf. appendix 2, page 9 ff. One of the providers, Fitbit, state in their terms of use that they will notify users by email or in the app, in the case of any material changes to their terms. Such reassuring notification is in itself welcome, but it is unclear what constitutes a material change and who determines what constitutes a material change. Mio are unclear as to whether they will give users advance notice of any changes, since the wording in their terms of use is non-committal on this point:

> "*we may notify you of any changes to this Privacy Statement via email and may ask you to affirmatively acknowledge consent to the changes"* (Mio PP)

The service providers also readily point out that users are bound by any changes to the terms of use made on the website. For example:

> "*Garmin may modify these Terms of Use at any time by updating this posting. You are bound by any such modification and should therefore visit this page periodically to review these Terms of Use*." (Garmin ToU)

To the Norwegian Consumer Council it is a cause for concern that the services do not give users satisfactory advance notice of changes to their terms of use. Failing to give notice could create an unfortunate lock-in effect, in that the user is prevented from exporting data and terminating their use of the service, and potentially also from finding a new provider, before the new terms come into effect.

There is reason to ask whether the failure to give advance notice, and the threshold for giving notice on the part of the service providers, could constitute an unreasonable term of use, and we urge the regulators to consider taking action. The Norwegian Consumer Council previously raised similar issues in their Apple complaint[16], which resulted in Apple making changes to their global terms of use in direct response to the Norwegian Consumer Council's complaint.

[16] http://www.forbrukerradet.no/wp-content/uploads/2015/10/Klage-på-brukervilkår-knyttet-til-Apples-iCloud.pdf

Data collection – how much data is collected, and how much is required to provide a functional service?

We have taken a closer look at whether each service provider collects more personal data than is necessary for delivering a functional service, including whether the service provider allows users to decline to the sharing of certain personal data with the provider. The latter is relevant if the service offers additional functions above and beyond its primary function (the registration of training activity over time), e.g. an option to register heart rate and sleeping pattern.

For example, all four providers require users to provide their full name and date of birth in order to use the service. One could ask whether this is a case of surplus information, especially since a significant amount of sensitive information is being collected and it is not clear which third parties the information is shared with. We ask whether it would be sufficient to ask for the year of birth in order to ensure than any age restriction for the service is observed.

Based on our review, cf. annex 2 page 12 ff., there is reason to believe that the service providers are in breach of the principle of data minimisation on this particular point, and we ask the regulators to investigate this.

Sharing personal data with third parties

Our review has found that the service providers' terms of use inadequately explain *which* third parties they share personal data with. This is problematic from a consumer perspective, as consent is required for such information sharing, something only one of the providers have provided for.[17] This is particularly problematic since it involves sharing data about heart rate and other activity data, which must be considered to be health data,[18] and which is deemed to be sensitive data by the law. Technical tests[19] have revealed that two of the activity wristbands submit information to Facebook when the user opens the associated app, irrespective of whether the user has actively linked the app to Facebook. This information allows Facebook to link a specific wristband to a specific user, amongst other things. The technical testing shows that one of the activity trackers sends the user's IP-address to two third parties that, as far as we can see, have targeted advertising as a part of their business model.[20]

The Norwegian Consumer Council asks whether the users' right to access and delete their personal data is rendered meaningless, since the service provider does not disclose whom the data is shared with.[21]

Deletion

The Personal Data Act and the Data Protection Directive place restrictions on the processing of data over time. Therefore, users must be given confirmation that data is deleted when they leave the service or are inactive for a period of time.

---

[17] Mio users do not have to share data; the app asks for your permission to share your data with it.

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf with annex http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

[19] The technical tests have not yet been completed, and a final report will be submitted in due course.

[20] Annex 3, page 6

[21] Personal Data Act Chapter III, Article 18 ff.

Our review of the terms of use found that none of the four services guarantees complete deletion of user data when an account is closed down. Fitbit stores copies of user data which is deleted "… *based upon an automated schedule"* without specifying exactly how the deletion procedure is designed with respect to the frequency of deletion of user data. Garmin will keep "[…] *residual information that will remain in our databases and other records, which will not be removed"*. It is unclear from this provision which data is involved, but as it is not possible for users to delete their Garmin account, we assume that at least usernames and email addresses will be stored. Mio allows users to delete "*certain personal information"* without explaining what this implies and also reserves the right to retain personal data for *"a period of time".* Jawbone's terms of use state that users may ask to have their data deleted but also that Jawbone will continue to use aggregated data.

The activity wristbands process sensitive data, and the Norwegian Consumer Council are concerned that none of the four service providers make it clear that user data is deleted when a user account is closed down. Nor do the terms of use say anything about procedures for deleting data associated with inactive user accounts. We find it particularly alarming that Garmin does not permit its users to delete their accounts at all.[22]

On the basis of the above, the Norwegian Consumer Council call for an investigation into whether the services meet the requirements stated in the Personal Data Act and the Data Protection Directive.

Notification of blocking and deactivation of user accounts

The terms of use for three of the four services include provisions allowing the services to unilaterally terminate or block user accounts. Advance notification is important to allow the user to respond to the alleged reasons for the deactivation. Being offered a portability option is also pivotal in such a situation.

In their terms of use, Fitbit state that *"[…] we reserve the right to deactivate your account or terminate these Terms, at our sole discretion, at any time and without notice or liability to you".* Jawbone follow the same principle, and reserve the right to remove user accounts without prior notice for any breach of its terms, including *"failing to provide Jawbone with accurate and complete Registration Data".* Garmin does not specify whether users will be notified in the event of deactivation or blocking. Mio's terms do not address blocking.

Portability

We note that the new General Data Protection Regulation defines portability[23] as a fundamental consumer right. Our study has found that full portability, with the option to both download and upload data, is not possible with the four services.

Fitbit, Jawbone, and Garmin all include functions allowing users to export their data. The file formats *.CSV* and *.XLS* are commonly used, and both Fitbit and Jawbone allow export in the former format. Garmin uses the formats *.TCX, .GPX* and *.FIT*. Only Garmin allows users to import fitness data, and then only in the three above-mentioned formats. In practice this means that you cannot upload exported data from Fitbit and Jawbone to Garmin's services. Neither Fitbit nor Jawbone offers an upload function, and Mio does not provide any form of data export/import at all.

[22] Annex 2, page 23

[23] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, article 20.

Making it impossible to move data presents an effective barrier from switching from one service to another if they so wish, e.g. if the terms of use are found to be unreasonable, because of functionality, etc.

Failure to provide portability creates a lock-in effect, and combined with the failure to give advance notice of deactivation we ask whether this constitutes an unreasonable term of use.

*

Our objections generally fall within the powers of the Norwegian Data Protection Authority, but they are also considered to be within the Norwegian Consumer Ombudsman's area of authority. The Norwegian Consumer Council is therefore submitting an identical complaint to both the Norwegian Data Protection Authority and the Norwegian Consumer Ombudsman, and urges them to jointly investigate the above objections.

The Norwegian Consumer Council awaits the investigation by the regulators, and would be happy to be of assistance if further clarification is needed.

Best regards
The Norwegian Consumer Council

Finn Myrstad
Head of section, Digital Services
Finn.myrstad@forbrukerradet.no

Appendix 1: Table with links to terms of use
Appendix 2: Report "*Consumer protection in fitness wearables*"
Appendix 3: Report "Investigation of privacy issues with Fitness Trackers" – v. 1.0 dated September 21st 2016