To:
The Norwegian Data Protection Authority
post@datatilsynet.no

Oslo 10.05.2016

Complaint concerning the mobile phone app Runkeeper

The Norwegian Consumer Council hereby lodges a complaint about issues relating to the mobile phone app Runkeeper:

1) Runkeeper tracks users and transmits personal data to a third party when not in use.
2) The app does not appear to delete personal data as a matter of routine or when the user requests it.

We would like to ask the Norwegian Data Protection Authority[1] to consider whether the Runkeeper app, owned by FitnessKeeper Inc., operates in compliance with Norwegian and European data protection laws and to determine whether the Authority is in a position to intervene.

FitnessKeeper Inc. is an American company based in Massachusetts[2]. As far as we know, the enterprise has no subsidiaries or representation in Europe[3]. FitnessKeeper Inc. is not registered under the Safe Harbour programme[4].

FitnessKeeper Inc. provides Runkeeper as an application (app). FitnessKeeper Inc. offers its services to the global market, including the European and Norwegian markets, and the company has associations with Europe in that it targets its services at the European market.

The app is available worldwide, including in the European and Norwegian markets. In the absence of any association with Europe beyond Runkeeper's being available in these markets, we acknowledge that the regulatory authorities' scope for imposing sanctions may be somewhat limited. Yet we are of the understanding that the Data Protection Authority may in certain instances be able to investigate cases such as this one. The Norwegian Consumer Council therefore asks that the Data Protection Authority use the channels available to it to look into the case and address the issues that it raises.

[1] www.datatilsynet.no
[2] FitnessKeeper, Inc., 2, 60 Canal St, MA 02114, USA
[3] FitnessKeeper is owned by the Japanese company Asics, best known for manufacturing trainers. Asics has representation in Europe.
[4] https://safeharbor.export.gov/list.aspx

Reason for the request

The Norwegian Consumer Council has studied the user terms and conditions and privacy policies of 20 different apps and presented its findings in a report[5]. The study looked in detail at certain/selected aspects of the apps' user terms and conditions and privacy policies that are of great significance to individual users. The study applied European legislation as a template for making comparisons and assessments.

During the review of the user terms and conditions and privacy policies, SINTEF carried out a test at the behest of the Consumer Council to analyse the actual data flow from the apps and to establish whether each app operates in accordance with its privacy policy[6]. SINTEF monitored data flow both when the apps were in use and when the mobile phone was idle for a period of 48 hours (the so-called 48-hour test). There were three apps in particular where we take the view that SINTEF identified breaches of privacy statements or terms and conditions[7]. They are Vipps (which the Data Protection Authority has already made contact with), Happn (which has been reported to the French data protection authorities), and Runkeeper, which we hereby bring to the attention of the Norwegian Data Protection Authority.

The Consumer Council's report shows that many apps, Runkeeper included, are not clear about what they define as personal data. Many apps, including Runkeeper, also request unreasonably wide-ranging permissions compared with the access actually needed to deliver the service. We have also noted that many apps, Runkeeper included, demand the perpetual right to the user's content, which includes a license to share the user's content to unspecified third parties. As many other app providers, Runkeeper also reserves the right to update their privacy at any time without prior notice. Seen in context of the wide-ranging licenses regarding user-generated content, the terms come across as unfair[8]. An additional issue we have identified in several apps, including Runkeeper, is that the service providers do not appear to delete personal data when the app has not been used for some time. Nor do they appear to delete data if a user deletes their user account.

About Runkeeper

Runkeeper is a fitness app. Users can keep track of how fast they and their friends are running, and they can see distances and maps of their own and their friends' training sessions. Users can also integrate the app with other apps such as Facebook and Spotify, and with fitness bands such as Fitbit[9].

[5] 'Appfail', The Norwegian Consumer Council 2016, http://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/ Link to the report on the Council's homepage.
[6] 'Privacy in mobile apps', SINTEF 2016 , http://www.forbrukerradet.no/undersokelse/2015/privacy-in-mobile-apps/
[7] This is addressed in the report 'Appfail', chapter 7 'Terms versus actual data flow'.
[8] http://ec.europa.eu/consumers/consumer_rights/rights-contracts/unfair-contract/index_en.htm
[9] See the Runkeeper website for more information – https://runkeeper.com/index

The service is very popular globally and is said to have around 45 million users. Runkeeper is one of the most popular fitness apps in Norway[10], although we do not have any figures as to the exact number of users.

The app generates extensive personal data, such as location in combination with time as well as information about the user's physical fitness, health and training habits.

Key documents regulating the legal relationship between app user and Runkeeper:
- *Terms of service* dated 21 December 2015: https://runkeeper.com/termsofservice
- *Privacy policy* dated 2 March 2016, effective 1 April 2016:
https://runkeeper.com/privacypolicy?showUpdatedPolicy=true

Objections
The Norwegian Consumer Council files a complaint specifically on the lack of consent regarding the collection and sharing of location data when the app is not in use, as well as the data deletion policies of Runkeeper. Regarding the issue of consent, we add that there is also fundamental problems regarding the unclear and wide permissions, with an opportunity to unilaterally change their terms without notice to their users. It could therefore be questioned whether there is actual informed consent when the app is installed and used, in addition to further changes to the policy by Runkeeper.

1) Runkeeper tracks users and transmits personal data to a third party when not in use

The study conducted by SINTEF found that Runkeeper collects location data and submits location data to a third party when the handset is not in use[11].

Location is a core function in Runkeeper's service and is as such relevant to the purpose of the app. A fitness app needs to obtain location data when the app is in use to allow the user to store training data.

However, we question why the fitness app collects location data and other personal information when the mobile phone and app are not in use. We also find it problematic that this personal data is transferred to a third party when the app is not in use.

We fail to see a need for obtaining such location information for functionality purposes, and would ask whether this is in line with the rules of purpose limitation. We therefore urge the Data Protection Authority to consider whether there has been a breach of the Data Protection Directive, which states that personal data may be collected provided it is reasonable and relevant in order to provide the service[12].

[10] http://www.dinside.no/928218/de-beste-lopeappene
[11] See the facts of the case described in the appendix.
[12] Article 6 of the Data Protection Directive (95/46/EC)

Runkeeper explains the technical permissions it requires. However, we cannot see that the app at any point – in the app itself, in the terms of use, privacy policy or on its website – makes the user aware that location or other personal data is collected when the mobile phone is not in use or when the user is not involved in a training session, nor that this data is forwarded to a third party.

The Runkeeper website describes access to location thus:

> ***'Location:*** *We hope this one is self-explanatory, but we do in fact use your location to track your workouts. The GPS hardware exists on your phone and Runkeeper needs this permission into* [sic] *order to use your phone's GPS so we can be your workout buddy on the road!'*
>
> Runkeeper, understanding permissions

As far as the user is concerned, it is therefore not self-explanatory that their location is tracked by fitness app and submitted to a third party when the user is not working out, when the app is not in use, or when the mobile phone is not in use.

Since this fact is not revealed, the user has not consented to personal data being collected when the app is not in use. We therefore ask the Data Protection Authority to consider whether this is a breach of the Data Protection Directive's stipulation that the user must give their explicit and informed consent to the collection of personal data[13].

Nor can we see that the user has consented to their location being forwarded to a third party when the app is not in use. We therefore ask the Data Protection Authority to consider whether this, too, is a breach of the Data Protection Directive's provisions on consent.

In this relation, we would like to make the Data Protection Authority aware that it seems that some information (such as IP-address and device identifier) shared with third parties, is not covered by the Runkeeper privacy policy, but by the policy of the third party, as disclosed in the Runkeeper privacy policy, chapter «Our Disclosure of Your Personal Data and Other Information»:

> *The use of online tracking mechanisms by third parties is subject to those third parties' own privacy policies, and not this privacy policy*

This suggests that Runkeeper does not take responsibility with information they share with third parties. Whether this also covers location data collected when the app is not in use is not clear.

2) It is unclear whether Runkeeper deletes personal data routinely or when the user requests it

According to the Data Protection Directive[14], controllers must limit the length of time they store and process personal data. Data may only be kept for as long as it is relevant. Apps such as Runkeeper

[13] Article 7 of the Data Protection Directive
[14] Article 6 of the Data Protection Directive

should therefore not continue to store personal data long after a user has stopped using the service, or when the user has asked for their account to be deleted.

From what we can see, Runkeeper's *privacy policy* or terms of service do not state whether there is a time limit on the data being stored or whether the service provider deletes personal data when the user requests it or deletes their account.

The *Runkeeper Help Center*[15] website provides information about how to use your personal Runkeeper account and about how to delete an account. On the page describing how to delete a Runkeeper account, users are informed that the data will be lost and that they will not be able to access this data once the account has been deleted. In other words, it does not say that the data is deleted, only that users will no longer have access to it.

The Norwegian Consumer Council would therefore like to ask the Data Protection Authority to look into whether Runkeeper satisfies the laws on privacy in respect of the deletion of personal data.

Best regards
The Norwegian Consumer Council

Finn Lützow-Holm Myrstad
Director of Digital Policy
Finn.myrstad@forbrukerradet.no

[15] https://support.runkeeper.com/hc/en-us/articles/201109826-How-to-delete-your-Runkeeper-Account

Appendix

Summary of findings made by SINTEF – the 48-hour test – Runkeeper

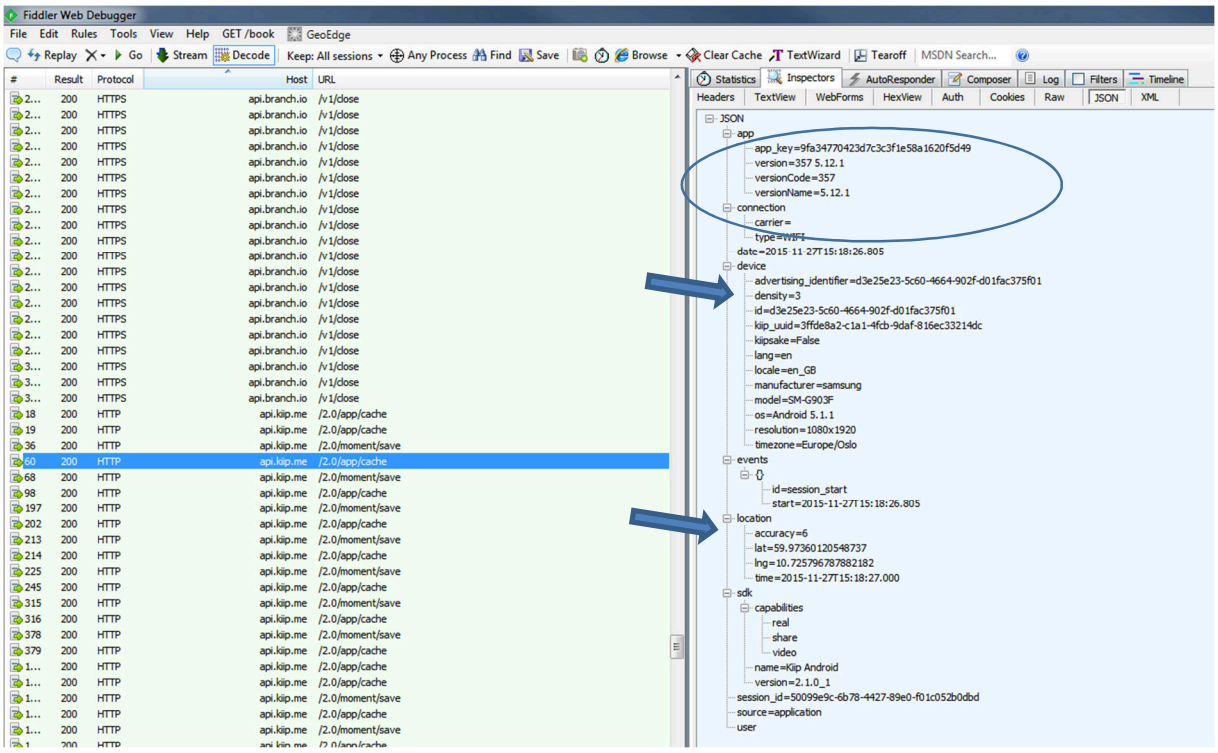
The SINTEF report concludes that Runkeeper submits the location when the handset is not in use:

> *'we also detected that GPS location was sent by MyFitnessPal and Runkeeper when the app was not in use. The user can then be geo-tracked whenever the GPS function is turned on'.*
>
> *Privacy in Mobile Apps, SINTEF,*

Background:

SINTEF found that the Runkeeper app submits personal data such as location combined with time and Google Advertising ID to the third party Kiip.me when the app is in use (see the data flow in screen dump 1) [16]. Using the location while the user is training is understandable in light of the app's functionality and is also described in the privacy terms, even though Kiip.me is not mentioned especially.

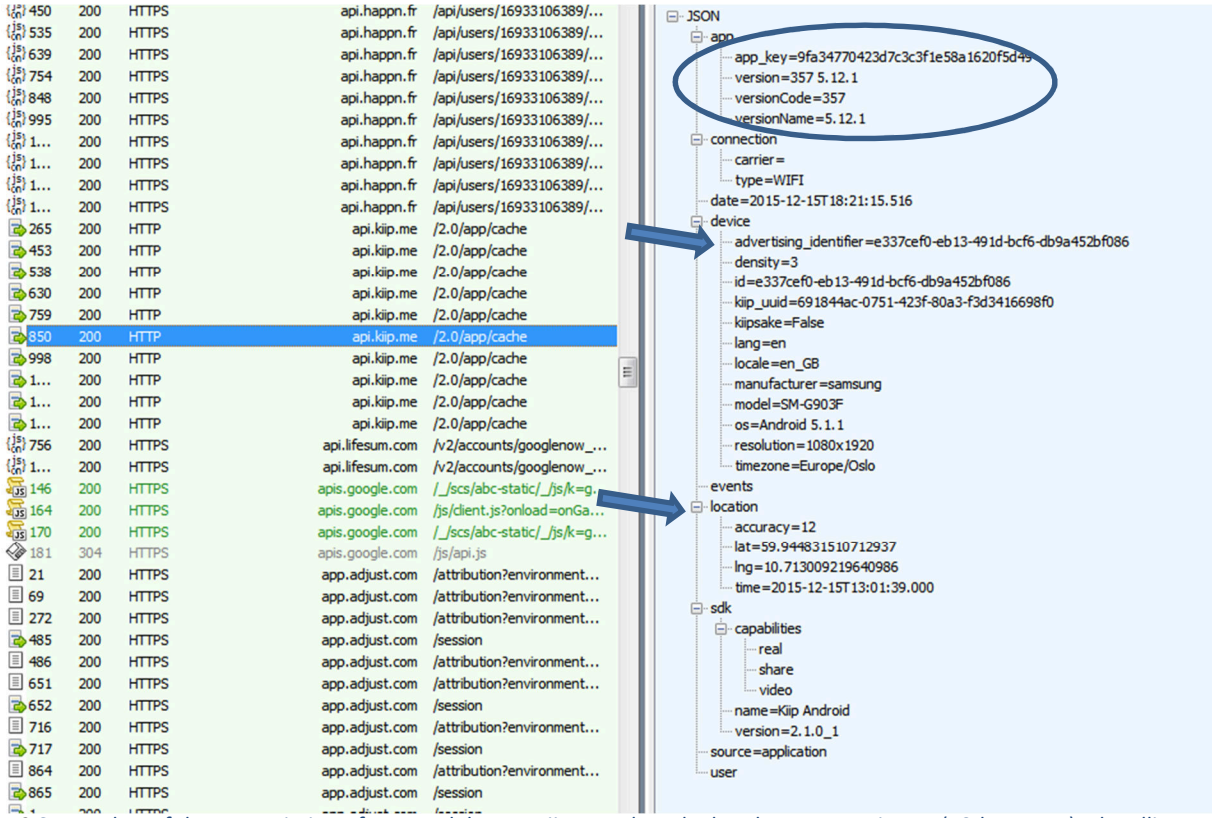
The Consumer Council has not assessed whether the forwarding of personal data to Kiip.me is problematic in itself. Yet we still mention that the data is sent to Kiip.me when the app is in use, because it has allowed us to ascertain that Runkeeper is sending personal data to a third party when the app is not in use.



[16] We have applied our interpretation of Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' when defining location and advertising ID as personal data.

1 Screen dump of data flow from Runkeeper while the app was in use. The ellipse shows app identifiers; the arrows show personal data.

SINTEF also found that one of the 20 apps sent a combination of personal data, including exact location, time and Google Advertising ID, to Kiip.me ten times during the 48-hour test. During the 48-hour test the mobile was not used for the duration of the 48 hours. (See screen dump documenting which data was sent to Kiip.me during the 48-hour test.)



2 Screenshot of the transmission of personal data to Kiip.me when the handset was not in use (48-hour test). The ellipse shows app identifiers; the arrows show personal data.

The submission of location and time 10 times over the course of 48 hours can in itself identify the user. The Google Advertising ID also constitutes personal data, since it is used as a permanent identifier until the user decides to actively change it – something few people do[17]. It is possible that other data, too, could be considered personal data, but we have not considered this as we deem it to be beyond doubt that personal data[18] has been transmitted.

[17] The reason why the Advertising IDs in the two screen dumps are not identical is that two different user accounts were used when testing the app while in use and while not in use.

[18] 'Even if the user periodically changes his or her pseudonymous GAID [Google Advertising ID], sparse trajectories—e.g., work-home location pairs—are known to be strongly identifying and allow the advertiser to link old and new GAID, effectively turning GAID into a permanent identifier.', 'What Mobile Ads Know About Mobile Users', 2016, Son, Kim & Shmatikov, page 8: https://www.ftc.gov/system/files/documents/public_comments/2015/09/00006-97209.pdf

SINTEF performed the 48-hour test with all 20 apps installed on the handset. We can conclude, however, that it was Runkeeper that transmitted personal data to the third party during the 48-hour test because of the app identifiers.

The data packages sent between Runkeeper and Kiip.me while the app was in use contained **app identifiers identical** to the data packages sent to Kiip.me when the mobile phone was not in use. They are 'app_key', which is a unique app identifier containing around 30 letters and numbers, 'version' (7 digits), 'versionCode' (3 digits) and 'versionName' (4 digits) (circled in screen dumps 1 and 2). Thus, we have demonstrated that the data was also sent through the Runkeeper app while the app was not in use.

Additional factors also point in the direction of Runkeeper being the app sending personal data to Kiip.me while the mobile phone was not in use. Runkeeper was the only **application that contacted Kiip.me** when SINTEF tested the applications one by one, and the only app in which SINTEF **detected Kiip.me source code**. SINTEF has also established that **Runkeeper used GPS while the mobile phone was not in use**.

Consequently, we believe it has been documented that Runkeeper sent personal data to a third party while the app and the handset were not in use.

We are happy to make further background information available to you if required. If so, please contact Gro Mette Moen on gmm@forbrukerradet.no.