

## SELECTION FROM DPA INVESTIGATION NIKE+ RUNNING APP

### CONCLUSIONS

The Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] has started an investigation into the processing of personal data by Nike in the context of the Nike+ Running app.

The company Nike Inc. from Beaverton, Oregon, the United States (hereafter: Nike), a famous manufacturer of shoes and sporting equipment, has created a number of fitness apps. Worldwide, the free Nike+ Running app has been downloaded to Android devices 10-50 million times. The Apple iPhone version of the app takes twelfth place on the list of most frequently downloaded fitness apps in the Netherlands.

The app helps people keep track of their running activities. The app can track distance, speed, time and number of calories burned. Users can use personal training programmes via the app to improve their performance. For these programmes, the app uses the GPS and network-based location data from the phone and the acceleration sensor (accelerometer). The app enables users to share their runs and photos with friends and enter competitions. Users must enter their height and weight in the app. This information is used to calculate the number of calories burned and, in combination with the gender and measurement data from the app, a user's stride length. Nike also calculates so-called 'Fuel points' - Nike's own metric for the level of exertion - based on measurement data from the app.

In order to be able to use the app, users using devices with the Android operating system are required to create a Nike+ account. In practice, the use of such an account is also convenient on devices with the iOS system (because of the backup and coaching options). When creating the account, users are obliged to enter their full name, gender, date of birth, postcode, country and email address. By creating the account, the data that are collected via the app on the phone are also passed on to Nike's servers and Nike can process these data for its own purposes.

#### *Controller*

Nike has its European head office in Hilversum, Nike European Operations Netherlands B.V. (NEON). The company Nike Retail B.V. is also located in Hilversum. Together, the two Dutch companies employ [confidential] people. Nike Inc., NEON and Nike Retail B.V. have submitted a joint notification to the Dutch DPA of their customer administration. In that notification, they indicated that they are jointly responsible for data processing via Nike's European website, that is to say for, among other things, the data processing via the Nike+ account and the sale of sports goods. From the notification to the Dutch DPA and from the Dutch DPA's investigation, it emerges that US-based Nike Inc. is the controller for data processing via the app, including the creation of the Nike+ account (but not for the purchase of goods via the online store and/or participation in events).

*(Special) personal data*

The data that Nike collects via the app (after the creation of a Nike+ account) are personal data as defined in section 1, under a, of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act]. Based on the user's height, weight and gender, Nike calculates an average stride length, tracks the stride length per running activity, and calculates the number of calories burned per walking or running activity. Nike stores these data in principle for an indefinite period of time.

In addition to this, for every runner, Nike records the (total) number of walking or running activities and (total) number of kilometres run (per half day, day, week, month and year). Nike also periodically calculates (in working memory) the average performance per user over time (everything, per week, month or year), the longest run and workout, the fastest kilometre run, the highest number of calories burned and 'trophies' achieved (certain achievements such as the number of kilometres run and milestones for Fuel points attained).

Nike can in any event conclude from this whether a user is sporty (runs frequently). For every data subject, Nike can see how often, how long and how intensively he or she runs (frequency, duration and intensity, measured via Fuel points). Nike can also draw conclusions as to whether the user is making progress, by, for example, covering the same distance, with a similar stride length, in a shorter period of time, whether or not in relation to the Fuel points achieved. Nike can conclude from this whether the data subject's condition is improving or deteriorating. This therefore involves processing data concerning health as referred to in section 16 of the Wbp.

Nike also categorises users worldwide into segments ('communities'). To this end, Nike selects users with reference to gender, age group, experience or running level. Nike then calculates the average sporting performance per segment, i.e.: Fuel points achieved, stride length, number of steps, number of running activities (per day, week, month and year), duration, calories burned, number of friends and total number of kilometres run for this category (distance).

Nike also makes at least one comparison of the individual sporting performance of a user against a calculated worldwide average for a comparable group of people (the total number of kilometres run). This comparison shows whether a data subject performs better, much better or worse than other individuals of the same age and gender. In addition to this, if a user has selected friends, Nike compares the total number of kilometres run with the same performance of friends.

Based on the same working method, Nike is technically able to also offer other comparisons, with regard to, for instance, Fuel points achieved, calories burned or stride length. The fact that Nike does not (currently) offer data subjects these other comparisons via the Nike+ account does not change the fact that Nike is technically able to make these comparisons per individual user. Nike can conclude from these comparisons how the condition of individual data subjects compares to comparable groups of people. Also via the calculation of average sporting performance and via the comparisons, therefore, Nike processes - via the app - data concerning the health of data subjects, as referred to in section 16 of the Wbp (after a data subject has created a Nike+ account).

The processing of health data entails risks, including the risk of unequal treatment based on an individual's presumed or actual health condition. This is therefore a processing of *special* personal data (data concerning the data subject's health) as referred to in section 16 of the Wbp. The processing of special personal data is prohibited unless one of the exceptions from articles 17 to 23 of the Wbp applies.

#### *Full disclosure obligation*

Nike informs (future) users in the Netherlands about the data processing via the app by means of two different privacy policies, a specific privacy policy for the app and a general privacy and cookie policy. Although there is no Dutch-language version of the app, both texts are also available in Dutch. Nike also provides information on the screen of the app and via its notification to the Dutch DPA.

During the Dutch DPA's investigation, Nike took measures to, for example, add missing references to the privacy policy. Nonetheless, Nike is (still) in violation of the provisions in sections 33 and 34 of the Wbp because information is lacking on the different types of personal data and the purposes of the data processing via the app.

#### Types of personal data

The privacy texts are wrongly lacking a clear overview of the types of personal data that Nike processes via the app. An explanation of the processing of health data is missing. Although Nike does mention in the privacy policy that it collects 'data about activities and performances' via the app, no explanation is included indicating that this involves an overview of an individual's sporting performance over time, including calculations of average and best performances, calories burned, stride length measured and Fuel points attained. Nor is any explanation given of the other types of data that Nike collects via the broadly-formulated consent requests on the smart phone. Because Nike also collects personal data via these authorisations (such as location data and email addresses), Nike must further inform data subjects about this on grounds of section 34 (3) of the Wbp.

#### Purposes of processing

The Dutch DPA has identified three purposes of the processing about which Nike must (still) inform data subjects, before Nike acquires the personal data:<sup>289</sup>

1. The tracking (on Nike's servers) of (developments in) the sporting performance of the individual.

---

<sup>289</sup> Idem, p. 68.

2. Comparison of the individual sporting performance against the average of a comparable group of people.
3. Research and analysis purposes

Nike does not inform data subjects, or informs them insufficiently, about these specific purposes of the processing.

Additionally, the Dutch DPA points out that the average data subject cannot be expected to understand that, if he or she creates an account via the app, the data are no longer contained only on his or her own device, but are also stored on Nike's servers, and that, consequently, Nike can also use the data for its own purposes. Nike must therefore inform data subjects about this in more detail, on grounds of the standard of due care that the controller must observe with respect to the data subjects.

In addition, the information in the privacy policy that indicates that Nike reportedly provides the data from the app and account only to processors is (still) inaccurate, as is the information in the cookie consent request on the website which indicates that no personal data are processed by advertising cookies.

#### *Exception to prohibition on processing health data*

Via the app, (after the Nike+ account is created) Nike processes special personal data (data concerning the data subject's health) as referred to in section 16 of the Wbp. The processing of special personal data is prohibited unless one of the exceptions from articles 17 to 23 of the Wbp applies. The only two exceptions on which Nike can rely are: express consent from data subjects or manifest public disclosure by data subjects.

Since Nike does not inform data subjects, or informs them insufficiently, about the types of personal data it collects and processes, and about the purposes of the data processing, Nike cannot rely on express consent from the data subjects for the two purposes investigated for which Nike processes health data.

With regard to the second exception, that *the data have manifestly been made public by the data subject*, the data subject must have had the express intention of making the data public and, according to the legislative history, this exception does not apply for data which a controller requests with a view to data processing. Neither exception applies in this case, therefore.

Although, during the Dutch DPA's investigation, Nike already made the reporting of the user's height and weight optional in new versions of the Running app (from the version of 10 June 2015 onward for Android and from 24 August 2015 onward for iOS), this measure does not change the fact that the health data of all existing users of the app are still being processed.

Because Nike (still) does not, via the versions of the Nike+ Running app investigated by the Dutch DPA, get express consent from data subjects to process data concerning their health, and because Nike cannot rely on one of the other exceptions to the statutory prohibition on processing, Nike is acting in violation of the provisions of section 16 of the Wbp by processing health data.

*Grounds for the data processing*

Nike stated that most of the processing operations for the functioning of the app and for its own commercial purposes in the context of the Nike+ Running app are based on the ground of unambiguous consent from the data subjects (as referred to in section 8, under a, of the Wbp). Nike also relies on express consent as an exception to the prohibition on processing special categories of personal data as referred to in section 23 (1), under a, of the Wbp. With regard to the processing of personal data for research and analysis purposes, Nike relies on the ground that the processing is necessary to uphold its legitimate interest (section 8, under f, of the Wbp).

Because the information that Nike provides to data subjects on the data processing falls short with respect to the different types of personal data that Nike processes via the app and the purposes for which these personal data are processed, the data subjects cannot give informed consent. Based on the current processes investigated by the Dutch DPA, therefore, Nike cannot rely on a ground under section 8, under a, of the Wbp for the processing of the other personal data that Nike collects and processes via the app (other than the health data).

This lack of unambiguous consent also applied (until November 2015) for the (inadvertent) placement/reading of a *tracking cookie* from Google DoubleClick when visiting the [nikeplus.nike.com](http://nikeplus.nike.com) website and for the pixel of Google DoubleClick in both app versions.

The Dutch DPA also tested the data processing against the grounds presented in section 8, under b and f, of the Wbp.

With regard to the need to process data in order to perform a contract, there may well be a ground to process location data with time/duration during the running activities, but this does not automatically mean there is a need to store these data for an indefinite period of time, or to analyse the use of the app with research questions such as ‘what is the best training plan?’ and ‘what is the best number of friends in the app?’ (to keep the use of the app going).

Nike has, in principle, a legitimate interest in processing the personal data (with the exception of the health data and the Google DoubleClick cookie) for the functioning of the app and for its own research and analysis purposes. There is a clear social demand for apps that help people with their running activities. Nike can only rely on this if it informs data subjects much more clearly and fully about the data processing that Nike itself performs, after the data have left the smartphone through the creation of an account. Nike's current processing, as investigated by the Dutch DPA, also does not (yet) satisfy the criteria of proportionality and subsidiarity. This is because Nike has not (yet) set a retention period for the personal data obtained via the app. Nike has saved all the data collected since the launch of the iOS app in 2010. The data are only deleted if a user actively deletes his account via Nike's websites. Nike still has no procedure for deleting inactive users of the app after a certain amount of time has passed.

In conclusion, because Nike does not obtain unambiguous consent for the investigated data processing via the app (after the creation of the account), it can only rely on the ground of section 8, under b, of the Wbp for a limited quantity of data for the functioning of the app and it cannot rely on section 8, under f, of the Wbp for the processing for research and analysis purposes, Nike is acting in violation of section 8 of the Wbp (with regard to the data which are not health data).

### **Measures announced**

In its written view on the report, Nike announced concrete measures to put an end to the remaining violations. These are summarised here:

- making changes to the cookie consent request on Nike's websites, so that a clearer distinction is made between (consent for) different types of cookies;
- making the reporting of height and weight optional also in the web environment of the Nike+ account (for users of the Running app who view their data via the website);
- informing existing users of the app by email that height and weight are optional and asking them [confidential] for consent to retain existing data;
- introducing a single privacy policy instead of the two texts currently used, in which more information is provided on the types of data that Nike processes and the different purposes of the processing. Nike also wants to devote more attention here to the fact that data from the app are saved on Nike's servers in the US (if a user has a NOERAIke+ account).
- the introduction of a retention period for inactive users [confidential].