Dutch DPA finds fitness app violates data protection law

The Dutch Data Protection Authority (College bescherming persoonsgegevens, hereinafter 'CBP') published a report on 11 November following an investigation into Nike's fitness app, the Nike+ Running app. The CBP found several violations of data protection law, according to its nearly hundred-page report. The report is interesting in that it provides detailed insight into how the Dutch Data Protection Authority views personal data concerning health and the thought processes behind the concept of health data, as Sofie van der Meulen and Erik Vollebregt of Axon Lawyers explain.

Violations of data protection law

Nike has developed an app specifically for runners with which they can track their activities: the Nike+ Running app tracks distance, speed, time and calories burned. Users can improve their performance with personal training programmes and compare their performance with other users. Although there is nothing wrong with these functionalities as such, the CBP found that informed consent should have been obtained from the users prior to the use of the app. According to the CBP's report, Nike violated data protection law on the following points:

- Nike does not provide sufficient information on what personal data are processed and for which purposes. Furthermore, Nike does not mention that the data are stored indefinitely.
- Nike processes health data through the app and has not obtained the required explicit consent from the user.
- Nike has no legal basis to process and use other information that is obtained from the smartphone, such as location information and contact information. Although Nike does inform users in more general terms about the processing and use of their data and asks for permission for the use of data, this information is not sufficient to establish informed consent. Based on the provided information, users are not able to determine the scope of the use of their data and cannot establish exactly what they give permission for. Therefore, there is no legally valid consent as a basis for the processing of personal data.

Does Nike process health data?

The Nike+ Running app is the first health app to be investigated by the CBP and the extensive report provides valuable guidance for similar fitness apps on the Dutch market in determining compliance with data protection law. Particularly the CBP's position regarding the concept of health data will be of interest to the mobile health ('mHealth') industry, as the current definition of health data is unclear.

The effect of practising sport on a person's condition: health data

In order to calculate distance, speed and time, the app uses the location data from the smartphone. For the calculation of the amount of calories burned and the length of a single step, users need to specify their gender, body length and weight. In addition, Nike calculates so-called 'Fuel-points,' a measure used by Nike to express the degree of effort made by the user. Nike periodically calculates the average performance of a user over time. From the start of use of the app an overview over time is created of all registered and calculated data for a specific user. Thus Nike has access to the sporting performance of a user over time. With this insight, Nike can conclude whether the physical condition of a user improves or deteriorates. According to the CBP, such information on a person's physical condition qualifies as health data as it provides information about the health of the user. The indefinite retention of the obtained data forms another factor to qualify the obtained data as health data because it allows a profile to be built up over time.

The deduced effect of practising sports on a person's condition: health data

Nike disagreed with the aforementioned conclusion of the CBP, as, according to Nike, there is no direct insight on the performance of a user on an individual level over time. Analysis of the data takes place on an aggregated level.

The CBP did not agree with Nike in this respect: even though analysis takes place on an aggregated level, Nike can still deduce whether a user is sportively active, based on the available information such as the frequency of the performed activities. Nike may also draw conclusions with regards to the progression achieved and thus deduce whether the condition of the person involved has improved or deteriorated.

In order to further explain its position, the CBP referred to scientific research showing that there is a direct relationship between exercise and life expectancy and the reduction of the risk of cardiovascular disease. How often and intensely a person exercises has a relationship with his/her life expectancy. Therefore, the data processed qualify as data

concerning health. The CBP argued that: "[the] captur[ing] of activities of users over time, with which the users can directly affect their life expectancy (positive or negative), should therefore qualify as processing of health data." Because Nike registers the running data over time, retains those data and is able to draw conclusions concerning a possible increase in life expectancy, the Nike Running app processes sensitive data concerning health as mentioned in Article 8 of the Data Protection Directive (Article 16 of the Dutch Data Protection Act). Nike may only process these sensitive personal data with the explicit consent of the user.

The CBP does not refer to a specific period of time to explain what is meant by "capturing user-data over time" which allows conclusions about a person's health to be drawn. This likely depends on the type of personal data collected and the personal data it is combined with and therefore should be assessed on a case-by-case basis.

New rules or new situation?

Nike argued that at the time of the investigation (early 2014) the definition of 'health data' was still unclear and that the CBP was not allowed to retroactively apply the criteria from the Article 29 Working Party ('WP29'), published in its letter of 5 February 2015. In this letter, the WP29 provided a number of criteria to assess whether the data collected by lifestyle and fitness apps are health data. The CBP stresses that the criteria from the WP29 do not constitute new rules. The CBP only applied the existing data protection law on a relatively new situation, namely the processing of health data through a fitness app.

Aside from Nike, there are numerous fitness, food and health app developers that may be similarly affected and in many cases have inadequate (or completely non-existent) privacy policies

The CBP on the concept of health data

The CBP further states that the concept of 'health data' must be interpreted broadly. Not only data processed in the context of a medical examination or medical treatment by a doctor, but also all data concerning a person's mental or physical health are covered by this concept. This broad concept is further substantiated by the legal history of Dutch data protection law, which shows that the additional controls on sensitive data do not only apply to data that directly shows a sensitive characteristic, but also to data from which a sensitive characteristic can be deduced. This approach is in line with the WP29 letter of February 2015 that provides examples of when the collected data, in combination, and certainly over time, leads to the processing of health data.

The WP29 states that: "For example, there are many apps available that enable users to register their weight and height, in order to calculate their body mass index. When the data are combined with a step counter, the data controller may use these data to infer whether the person has a sedentary way of life or not. Combining these data, the data controller may qualify some users as part of a population with increased health risks. […] Clearly, these types of data processing deserve significant attention. If data are health data, but mistakenly treated as 'ordinary' personal data, there is a risk that the high level of protection deemed necessary by the European legislator is undermined."

The impact?

The CBP has only assessed the Nike+ Running app, its related notification procedures and privacy policies. Nike has already taken measures during the time of the investigation to end some violations, implemented improvements and has announced further measures to ensure compliance in the future. The CBP will monitor the actions taken by Nike and check if all the reported violations have come to an end. Aside from Nike, there are numerous fitness, food and health app developers that may be similarly affected and in many cases have inadequate (or completely non-existent) privacy policies. A general text such as 'We will not use your health data for marketing purposes' is not sufficient to be compliant. The user has to be fully informed about the purposes of data processing and how the data is used. All data that is collected has to be spelt out in the privacy policy. To date, the CBP has not looked into other fitness and health apps. According to the reasoning of the CBP however, apps that let you keep track of what you eat (such as food diaries) actually handle health data. The same is true for apps that capture the activities of people over time, which may directly affect persons' life expectancy (positive or negative). Also in the case of a food diary a link can be established between food, health and life expectancy. Whether data protection authorities in other Member States will uphold the position of the CBP with regards to the concept of health data remains to be seen, but in the light of the WP29 letter of February 2015 this is not unlikely at all.

Sofie van der Meulen Lawyer
Erik Vollebregt Lawyer
Axon Lawyers, Amsterdam
sofie.vandermeulen@axonlawyers.com
erik.vollebregt@axonlawyers.com