When is It Health Data and When is It Not?

Data about a person's health is a special category of data which requires a higher level of data protection than many developers of health-related apps and devices are aware of. Moreover, it is not always obvious when data becomes health data. We share the highlights from a new guidance from the Working Party on the subject.

By Thomas Bjørn and David Hobson

Over the past years, we have seen a rapid growth in the market for health and fitness-related apps and devices, covering a large variety of fields of use, with recent examples ranging from general warning systems tracing the development of infectious diseases and platforms for app developers like Apple HealthKit over downloadable mobile apps to medical devices for professional use.

The common feature shared by most of these developments is the collection of data which regularly includes personal data.

Data protection has become an issue of increasing importance in the digital era. If the personal data collected by apps and devices are classified as health data, then they have to be appropriately protected and can only be processed if the data subject "unambiguously" gives his consent which must be clear, knowingly given and limited to a specific purpose.

But when is it health data ?

For developers and users of the rapidly increasing number of health-related apps, this is a very important question and an issue on which legal certainty is required. At the request of the European Commission, the Working Party has therefore recently published guidance regarding the use of health data which provides some warnings but also useful advice to developers and operators of apps and devices.

3 Types of Health Data

Article 8 of the Data Protection Directive (95/46/EC) classifies health data as a special category of data which requires a higher level of data protection. The processing of such data is generally prohibited, unless an exception applies such as the express consent of the data subject.

The Directive, however, does not offer a definition of "health data" – it merely lists the term together with other "special categories", so up to now it has been unclear what the term actually means.

As a result, the numerous providers of health and wellbeing apps and devices may have been at risk of processing data in breach of the Directive and its implementation into national law. It is therefore helpful that the Working Party has now offered some guidance as to the kind

ABOUT THE AUTHORS


THOMAS BJØRN works as a solicitor with Royds LLP in London. His areas of expertise include the protection and commercialisation of intellectual property, regulatory affairs and the sale of goods and services to the NHS. Royds LLP is a London City based law firm providing legal services to the international business community. The firm specialises in commercial law and has a strong focus on intellectual property and the life science industries.

DAVID HOBSON is a part-qualified patent attorney at Mathys & Squire, which is one of Europe's most established and renowned specialist IP firms, with specialist attorneys in a wide range of technical fields including biotechnology, phamacology, eletronics, engineering and more. David Hobson has experence of drafting and prosecuting UK, European and foreign patent applications for at wide range of technologies pertaining to the field of biotechnology.

of data covered by the term.

The guidance makes it clear that health data can be classified into three categories:

- Data that are inherently/clearly medical data;
- Data that are raw sensor data that can be used alone or in combination with other data to draw a conclusion about the actual health status or health risk for a person; and
- Conclusions – whether accurate or not – about a person's health status or health risk.

The term includes the obvious health data, i.e. data about the physical or mental health status of an individual, their medical history, diagnosis and treatment, together with any data generated by apps or devices which are used in this context. However, at its broadest interpretation the guidance concludes that health data can be seen to be any data about an individual that can be associated with a condition or allow some kind of diagnosis or inference about health status.

For example, data encompassed by this definition could include (amongst others) information about a person's drinking or smoking habits, membership of patient support groups or use of corrective glasses .

Clearly, this has important ramifications for health and wellbeing application developers who must strive to ensure that such data is protected in accordance with the relevant EU directives and national law.

At the other end of the spectrum, the Working Party recognises that there are categories of data generated by apps and devices which must be classified as raw, low privacy impact personal data. As an example, the guidance mentions an app counting the number of steps during a single walk or making a single registration of a person's weight, blood pressure or pulse. As no interpretation of the health status of the data subject can be made from such data, they cannot be classified as health data. It is, however, important to note that such low-impact information can very easily change into health data. If distance walked, weight and pulse are measured over time and/or used in combination with other information including diet, age, sex or even location data, it will be

possible to draw conclusions about the health status of the data subject. If such conclusions can be drawn, the data will – regardless of whether the conclusions are correct or not – be regarded as health data and will be subject to the general prohibition in Article 8 of the Directive. The guidance recognises that for the functioning of some health apps it will not always be necessary to transfer the data off the device.

If the data processing takes place on the device itself and no personal data are transmitted outside the device, the processing will be covered by Article 3 (2) of the Directive and will therefore be exempt from the legislation.

If It is Health Data You Need Explicit Consent

If the operator of the app or device (the data processor) collects data which amount to health data as defined above, he can only do so by relying on one of the exemptions in Article 8. In relation to the processing of health data from apps and devices, the relevant exemption is consent. Article 7 (a) requires that the data subject "unambiguously" gives his consent which must be clear, knowingly given and limited to a specific purpose. This is highly burdensome, both for the data processor and for the data subject.

The guidance provided by the Working Party is much needed given the growth in popularity of health and wellbeing apps, devices and wearable technology, with an expectation of further growth in the coming years. The guidance also reveals new challenges for health and wellbeing application developers who must ensure the appropriate protection, responsible processing and storage of health data belonging to data subjects. The question is whether or not such requirements are realistic in the digital era – but that is another discussion. The Article 29 Working Party is composed of representatives from the data protection authorities of the EU member states and acts as an independent European advisory body on data protection and privacy.

Although not legally binding, the opinions of the Working Party are regularly referred to in legal decisions in the member states.