February 2015

Article 29 Working Party Clarifications on the Scope of Health Data Processed via Lifestyle and Well-being Apps

On February 5, 2015, the Article 29 Working Party (the "Working Party") published a letter that responds to a request of the European Commission to clarify the scope of the definition of health data in connection with lifestyle and well-being apps. In the annex to this letter, the Working Party identifies criteria to determine when personal data qualifies as health data, a special category of data receiving enhanced protection under the EU Data Protection Directive 95/46/EC (the "Directive"). The Working Party further discusses the current legal regime for the processing of health data and provides its view on the requirements for further processing of health data for historical, statistical and scientific research under the Directive. The Working Party also provides recommendations on how these topics should be addressed in the proposed EU General Data Protection Regulation (the "Proposed Regulation").

Scope of Health Data

The Working Party identifies three main scenarios where personal data processed via lifestyle and well-being apps and devices is considered health data:

- Data processed via the app or device is inherently/clearly medical data;
- Raw sensor data processed via the app or device can be used, independently or in combination with other data, to draw conclusions about an individual's actual health status or health risks; and
- Based on data collected via the app or device, conclusions are drawn about an individual's health status or health risks (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate or otherwise adequate or inadequate).

The Working Party has given a broad interpretation to the concept of health data, which is certainly not limited to "medical data" in the strict sense (i.e., data about an individual's physical or mental health status generated in a professional medical context, including data generated by apps or devices used in this context). It includes all data pertaining to an individual's health status, regardless of the context in which it was collected and regardless of whether the information establishes "ill health." The Working Party refers to the definition of health data in the Proposed Regulation to clarify that information derived from the testing or examination of a body part or bodily substance (for example, information generated by devices analyzing an individual's urine or blood or apps monitoring an individual's blood pressure or heart rate), information about disease risks (i.e, any information on an individual where there is a scientifically proven or commonly perceived risk of future disease, such as drug use, excessive alcohol consumption, etc.) and information about the actual physiological or biomedical state of an individual independent of its source, also fall within the category of health data.

In addition to information considered as health data due to its nature, certain data processing activities may be considered by the data protection authorities as processing of health data due to the way they are performed. In this respect, processing seemingly innocuous information could be considered as processing of health data where it entails tracking of information over time, combining it with other data or disclosing it to other parties having access to additional information concerning the individual, in

particular where such processing is done for profiling or direct marketing purposes. Combining nonsensitive information concerning an individual's height and weight collected through an app for BMI calculation, with information from a pedometer to assess increased disease risk would, for example, qualify as health data processing. However, for such processing to qualify as health data processing, there has to be a demonstrable relationship between the data collected through the app or device and the capacity to determine a health aspect of an individual, based on the data itself or in combination with other information. Information generated by a pedometer app that counts an individual's steps only during a single walk without being able to combine this with other information will, for example, not qualify as health data.

Legal Requirements for Processing Health Data

In addition to identifying which data should be considered health data, the Working Party has also clarified the requirements that should be taken into account when processing such data.

First of all, the Working Party takes the position that the requirements of the Directive do not apply when the data processed by lifestyle and well-being apps is not transmitted outside the user's device. However, if the data is transmitted outside the device and it qualifies as health data, its processing is allowed only in limited cases (listed in Article 8 (2), (3) and (4) of the Directive). Unless data is processed in a strict medical context (implying processing by individuals subject to professional secrecy obligations for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health care services), the Working Party is of the opinion that explicit consent will most likely be required to legitimize the processing. According to the Working Party, consent will be required in any event (regardless of whether it concerns health data or not) in case the well-being or lifestyle app or device processes location data or other data collected through sensors on an individual's mobile device.

Apart from ensuring that there is a legal basis, app and device developers and providers should also comply with the other key requirements of the Directive. The Working Party stresses the importance of providing clear and easily accessible information to the users before they install an app or purchase a device. It should be clear to users whether their data will be protected by medical secrecy, whether the data will be combined with other information stored on the device or collected from other sources, for which purposes the data will be further processed (if any) and to whom it may be disclosed. Without this prior information, the users' consent risks to be deemed invalid.

The Working Party also underlines the need to define clear, compatible and legitimate purposes for the data processing, as well as the requirement to implement proper anonymization techniques and other risk-reducing measures, such as privacy by design and data minimization.

Further Processing of Mobile Health Data

The Working Party also confirms its view with respect to the ongoing debate concerning the regime for further processing (or "secondary use") of health data under the Proposed Regulation.

The Proposed Regulation amended by the European Parliament introduces strict consent requirements for the further processing of health data for historical, statistical or scientific research purposes, which would also apply to data collected via apps and mobile devices. In addition, the European Parliament has proposed exceptions to these consent requirements, if the research serves high public interests, cannot possibly be carried out otherwise, and other safeguards are applied. The Working Party endorses these amendments, as they are deemed to give individuals more control over their private life. However, the Working Party is concerned about the notion of a lighter data protection regime for "pseudonymized" (i.e., encoded) personal data, particularly in the context of research. Since the European Parliament added a definition of "pseudonymous data" to the Proposed Regulation, there has been much discussion about the status of personal data that has been pseudonymized. According to the Working Party, pseudonymized data cannot be considered equivalent to anonymized data. Therefore, the use of pseudonymous or pseudonymized data is, in itself, not sufficient to justify a lighter data protection regime. The Working Party also encourages the European Commission to make a clear statement that further

processing of health data collected via apps and mobile devices generally requires explicit consent — even if the data is pseudonymized — unless national law exceptions apply.

Contacts

Global Privacy and Cybersecurity

Wim Nauwelaerts
wnauwelaerts@hunton.com

Bridget Treacy
btreacy@hunton.com

David Dumont
ddumont@hunton.com

Life Sciences

Prof. Lucas Bergkamp
lbergkamp@hunton.com

Gary C. Messplay
gmessplay@hunton.com

Geneviève Michaux
gmichaux@hunton.com

Tim Hickman
hickmant@hunton.com