ANNEX - health data in apps and devices

Concept of "health data" in Directive 95/46/EC

Article 8 of the Data Protection Directive (95/46/EC) qualifies health data as a special category of data to which a higher level of data protection applies. The Processing of special categories of data is prohibited, unless an exception applies. In its advice paper from 2011 to the European Commission the Working Party has explained the rationale behind this stricter legal regime.[1] It stems from the presumption that misuse of these data in general, is likely to have more severe consequences for the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "less sensitive" types of personal data. Misuse of health data, including drawing incorrect or unreliable conclusions, may be irreversible and have long-term consequences for the individual as well as his or her social environment.

The Data Protection Directive thereby sets a high level of protection for health data, but does not define clearly what type of information must be regarded as health data within the meaning of Article 8. Defining the category of health data is important to determine in what circumstances the data processed by lifestyle and wellbeing apps and devices are to be considered data about health.

Defining health data

In its advice paper, the Working Party remarked that, due to the wide range of personal data that may fall into the category of health data, this category represents one of the most complex areas of sensitive data and one where the Member States display a great deal of diversity and legal uncertainty.

In its proposal for a data protection Regulation[2] the European Commission has proposed (unchanged by the European Parliament[3]) the following definition in Paragraph 26 of the Preamble:

Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

---

[1] Article 29 Working Party, Advice paper on special categories of data ("sensitive data"), April 2011, URL:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

[2] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, 2012/0011 (COD).

[3] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), unofficial consolidated version after LIBE committee vote, provided by the rapporteur
22 October 2013.

The Working Party takes as a starting point that there is a category of information which is uniformly considered as health data. This is the category of medical data, the category of data about the physical or mental health status of a data subject that are generated in a professional, medical context. This includes all data related to contacts with individuals and their diagnosis and/or treatment by (professional) providers of health services, and any related information on diseases, disabilities, medical history and clinical treatment. This also includes any data generated by devices or apps, which are used in this context, irrespective of whether the devices are considered as 'medical devices'.

But health data (or *all data pertaining to the health status of a data subject*) is a much broader term than the term 'medical'. Based on the current Data Protection Directive, national legislators, judges and DPA's have concluded that information such as the fact that a woman has broken her leg (Lindqvist), that a person is wearing glasses or contact lenses, data about a person's intellectual and emotional capacity (such as IQ), information about smoking and drinking habits, data on allergies disclosed to private entities (such as airlines) or to public bodies (such as schools); data on health conditions to be used in an emergency (for example information that a child taking part in a summer camp or similar event suffers from asthma); membership of an individual in a patient support group (e.g. cancer support group), Weight Watchers, Alcoholics Anonymous or other self-help and support groups with a health-related objective; and the mere mentioning of the fact that somebody is ill in an employment context are all data concerning the health of individual data subjects.

The category also includes health related data used in an administrative context, such as data disclosed to public bodies on whether one’s household includes individuals with specific diseases and/or disabilities for the purpose of tax deductions or other allowances. Last but not least, the category also includes data about the purchase of medical products, devices and services, when health status can be inferred from the data, or information about the participation in some selectively performed screening tests (e.g. screening for AIDs or other sexually transmitted diseases, or rare diseases).

For data to qualify as health data it is not always necessary to establish 'ill health'. For example in the case of blood or urine tests, performed in order to diagnose someone's health, the detailed results of such a test qualify as health data, irrespective of whether the results are all within the 'healthy' limit or not. This also applies to data collected in the context of online questionnaires with the purpose of providing health advice, regardless of the input the data subject provides.

The broad scope of the term health data is reflected in the proposed definition in the Regulation. According to the proposed definition, health data also include: 'information derived from the testing or examination of a body part or bodily substance, including biological samples' and: any information about 'disease risk' and about 'the actual physiological or biomedical state of the data subject independent of its source'. This may include devices analysing a person's urine and blood, and apps measuring blood pressure or heart rate, regardless whether the testing is performed by medical professionals or by devices and apps freely available on the commercial market and irrespective whether these devices are marketed as medical devices or not. A clear example of such medical health data is a glucose metering app that warns if the glucose level is too high and advises the user to take action.

The term 'disease risk', mentioned in the proposed definition, refers to data concerning the potential future health status of a data subject. According to the Working Party, health data therefore also include information about a person's obesity, high or low blood pressure, hereditary or genetic predisposition, excessive alcohol consumption, tobacco consumption or drug use or any other information where there is a scientifically proven or commonly perceived risk of disease in the future.

In addition this may also include cases where a controller uses any personal data (health data or not) with the purpose of identifying disease risks (such as, for example, investigating exercise habits or diet with the view of testing new, previously unknown or unproven correlations between certain lifestyle factors and diseases). This may often be the case in medical research using big data.

On the other side of the spectrum, the Working Party assumes there is a category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as health data within the meaning of Article 8. This concerns data from which no conclusions can be reasonably drawn about the health status of a data subject. Not all raw data collected through an app (measurements) qualify as *information* (from which meaning can be derived) about the health of a person. For example, if an app would only count the number of steps during a single walk, without being able to combine those data with other data from and about the same data subject, and in the absence of specific medical context in which the app data are to be used, the collected data are not likely to have a significant impact on the privacy of the data subject and do not require the extra protection of the special category of health data. They are just raw (relatively low impact lifestyle) personal data (provided, the app does not process location data), not information from which knowledge about that persons health can be inferred.

How to deal with grey areas

There remain some types of processing, where it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data. This is especially the case where the data are processed for additional purposes and/or combined with other data or transferred to third parties. These types of data processing may create risks, including the risk of unfair treatment based on data about a person's assumed or actual health status.

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. If seemingly innocuous raw data are tracked over a period of time, combined with other data, or transferred to other parties who have access to additional complementary datasets, it may well be that even the seemingly most innocuous data, combined with other data sources, and used for other purposes, will come within the definition of 'health data'.

This risk specifically applies to further processing of such data for profiling and marketing purposes, given that the key business model of most apps is based on advertising.

When the personal data collected through an app or device are health data, the possibilities for further processing for different purposes than for the provision of professional health care are very limited.

The privacy risks associated with the processing of health data within the meaning of Article 8, must be assessed against the rapid technological developments in mobile and wearable technology and the increasing popularity of 'quantified self' apps and devices, that allow people to register all kinds of aspects about their personality, mind, body, behavioural patterns and whereabouts. In combination with other data, these data can be used to draw conclusions about the health of the data subjects using the apps and devices and treat them differently, in helpful and positive, but also in negative and/or unexpected ways. An example of such further processing is analysis conducted on social media to detect whether people may suffer from a depression. Even though 'sad' messages sent by users, in general, do not have to be treated as health data by (generalist) social networks, the systematic analysis of such messages for the purpose of diagnosis/health risk prevention or medical research certainly qualifies as the processing of health data.

With these apps, it is not only the user that collects data about himself or herself. Frequently, the information is (also) processed by a data controller. It is critical that users can consciously determine whether they consent or not to any (further) processing of data from which conclusions may be drawn relating to their health. 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. If the data controller does not clearly inform users of the app about the purposes of the processing, users may wrongfully assume that all their data stay on their own device, for their own use only. Or, in the case of an app aimed at people with diabetes; it can be very useful for the patient to share the most recent glycaemia levels with his or her doctor, but there are clear risks if such sharing also leads to further processing by other parties. Therefore, as this type of data processing is not easy to recognize as the processing of health data, but at the same time brings with it real privacy risks, it is important to provide a set of criteria that help determine in which cases lifestyle data should be treated as health data within the meaning of Article 8.

Examples of possible indicators that health data are processed

Raw, relatively low privacy impact personal data can quickly change into health data when the dataset can be used to determine the health status of a person. To assess this, it does not suffice to look at the character of the data as is. Their intended use must also be taken into account, by itself, or in combination with other information. For example, a single registration of a person's weight, blood pressure or pulse/heart rate (if not excessive in absolute terms), at least without any further information about age or sex, does not allow for the inference of information about the actual or likely future health status of that person. However, that aspect measured over time, especially in combination with age and sex, may be used to determine a significant aspect of an individual's health, such as the health risks related to obesity or an illness causing a significant loss of weight, high/low blood pressure, arrhythmia etc.[4] A significant loss of weight may be due to several reasons, some positive (a drastic diet), some negative (impact of a harsh medical treatment; depression, etc.). It is critical to underline that this type of information is not neutral. When conclusions are drawn about someone's health, regardless of their reliability, these conclusions are to be treated as health data.

There has to be a demonstrable relationship between the raw data set and the capacity to determine a health aspect of a person, based on the raw data itself or on the data in combination with data from other sources. For example, if a diet app only counts the calories as calculated from input provided by the data subject, and the information about the specific foods eaten would not be stored, it would be unlikely that any meaningful conclusions can be drawn with regard to the health of that person (unless the daily intake of calories is excessive in absolute terms). But if data from a diet app, or heart rate monitor or sleep diary app are combined with information provided by the data subject (directly or indirectly, for example based on information collected from that person's social networking profile), conclusions (whether accurate or inaccurate) may be drawn about that person's health condition, such as medical risk or diabetics. In these cases it is likely that health data can be inferred from the combined data.

[4] See also Article 29 Working Party, WP 223, Opinion 8/2014 on the *Recent Developments on the Internet of Things*.

Raw sensor data thus may lead to the drawing of conclusions (whether accurate or inaccurate) concerning the health status of a data subject. Such conclusions are health data, even though the raw sensor data may not always be.[5]

In summary, personal data are health data when:

1. The data are inherently/clearly medical data
2. The data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person
3. Conclusions are drawn about a person's health status or health risk (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate)

Domestic exception

It may not always be necessary for lifestyle and wellbeing apps to transmit any data outside of the device. If the data processing only takes place on the device itself, and no personal data are transmitted outside the device, the law wouldn't apply to the user, because of the exception for purely personal use, as laid down in Article 3 (2) of the Data Protection Directive 95/46/EC.[6]

Legal ground: explicit consent

If the data controller collects data through the app or the device, and it concerns apps with a medical purpose (e.g. apps through which patients can share data on symptoms and compare which treatments work best for them; apps that contain reminders to take medication; personal data tracking, science, and collaboration apps to help both medical research and individuals to understand how their body works and make healthier choices), or where health data can be reasonably inferred from the data tracked by the application (e.g. apps to track food and exercise in an effort to lose weight; body fat monitor and scale used for the same objective; apps that allow you to find correlations between your individual data streams, like how your diet correlates with your sleep and your mood), the data controller needs to be able to rely on a derogation from the general prohibition in Article 8 (1) of the Data Protection Directive of the processing of personal health data. The Directive provides for mandatory derogations laid down in Article 8 (2) and (3) plus an optional exemption in Article 8 (4). With regard to apps and devices that allow for the inference of health data the most likely derogation is explicit consent, as laid down in Article 8 (2)(a) of the Directive.[7]

---

[5] When raw data should be considered health data is also a matter of scale: a pedometer tracking and storing how many steps one has taken for a few days (and deleting such data after a week by default) may not process 'health data'. But an app combining several years' worth of extensive quantified-self records of an individual (tracking, for example, sleep and exercise habits, detailed records of diet, weight, body mass index, blood pressure and other vital statistics, as well as a mood diary) will be processing health data. Importantly also, in this latter case not only the conclusions and inferences, but also the raw data will be considered health data.

[6] In case the data controller provides for a remote platform where the data are collected and processed, it is important to note that the domestic exception only applies to the actual usage by the user him or herself and does not exempt the data controller from his responsibilities under data protection law for the processing for his own purposes. See Article 29 Working Party, WP163, Opinion 5/2010 *on online social networking* and Article 29 Working Party WP 223, Opinion 8/2014 on the *Recent Developments on the Internet of Things*, p. 13

[7] Explicit consent is not required for the processing of data concerning health by persons subjected to professional (medical) secrecy obligations, if the processing is required for preventive medicine,

Many lifestyle apps and devices also process location data and read data collected through one or more sensors on a mobile device. Even if the wellbeing data collected through the app are not to be regarded as health data, because a person's health status cannot be determined from the data, the combination with location data or other information read from the device would still make it necessary for the data controller to obtain the unambiguous consent of the data subject, as laid down in Article 7(a) of the Directive, in combination with Article 5(3) of the ePrivacy Directive.[8]

Transparency, purpose limitation and security

Without repeating earlier opinions of the Article 29 Working Party on the key provisions of data protection law, [9] and specifically the opinion on apps on smart devices, it is important to note that the principle of transparency is inseparably connected to the legal ground of consent. Without clear and prior information about the well-defined purposes of the processing, users are unable to provide legitimate consent.

The data controller must clearly inform users whether the data are protected by any medical secrecy rules, or not. Further information must be made available whether the data will be combined with other data stored on the device or collected from other sources and clear examples of the consequences of such combination of data, what the purposes are of further processing and to what third parties the data may be transferred. Such information must be made available in a clear and easily accessible manner before users decide on installing apps or buying devices (also before downloading the app).

Purpose limitation is another key provision that deserves careful consideration. When the processing involves health data, further processing for different purposes (outside the professional health care domain) is strictly limited. The data controller must define clear compatible and legitimate purposes of the data processing. This is an essential guarantee against the risks of misuse of the data.[10]

Last but not least, the Working Party refers to its advice to apply proper anonymisation techniques[11] and other security measures, including privacy by design and data minimisation, as outlined in its opinion on apps on smart devices.[12]

Future developments with regard to health data

In view of the discussions about the proposed Data Protection Regulation, the Working Party wishes to provide some additional reflections about the further processing of health data, for historical, statistical and scientific research purposes.

---

medical diagnosis, the provision of care or treatment or the management of health-care services, as laid down in Article 8 (3) of the Data Protection Directive.

[8] See also Article 29 Working Party, WP 185, Opinion 13/2011 on *Geolocation services on smart mobile devices*. The only applicable legal ground for the processing of patterns of location data is the unambiguous consent of the data subject.

[9] See Article 29 Working Party, WP 223, Opinion 8/2014 on the *Recent Developments on the Internet of Things,* WP 217 Opinion 06/2014 on *the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 187, Opinion 15/2011 *on the definition of consent* and WP 136, Opinion 4/2007 on *the concept of personal data*.

[10] See also: Article 29 Working Party, WP 203, Opinion 03/2013 *on purpose limitation*.

[11] Article 29 Working Party, WP 216, Opinion 05/2014 *on Anonymisation Techniques*,

[12] Article 29 Working Party, WP 202, Opinion 02/2013 *on apps on smart devices*, p. 18-21.

As the Commission notes in its Green Paper, mHealth can facilitate the mining of large amounts of health data. The Paper mentions that personal sensor data are expected to grow from 10% of all stored information to approximately 90% within the next decade. While these data are said to be able to contribute to epidemiological research, to the reduction of trial periods for medication or to the development of mechanisms for the detection and prevention of diseases, the further processing of these data needs to comply with data protection requirements. According to the Commission, this raises the ethical issue of obtaining explicit specific and informed consent. The Working Party agrees with this analysis.

In response to the European Commission proposal for a General Data Protection Regulation, the European Parliament has adopted highly significant changes to the exceptions for further processing of (amongst others) health data. In Article 81 the European Parliament proposes to introduce a strict consent requirement from data subjects for the processing of personal health data which is necessary for historical, statistical or scientific research purposes. Simultaneously, the EP has also proposed exceptions to this requirement of explicit consent, if the research serves high public interests, cannot possibly be carried out otherwise, and other safeguards are applied. Furthermore, the EP has added a right to object to such further processing.

In principle, the Working Party welcomes and endorses these amendments, as they will give data subjects enhanced control over the use of very intimate details about their private life. The Working Party recalls its *Statement on the role of a risk-based approach in data protection legal frameworks* of 30 May 2014, where it has underlined that fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. The Working Party simultaneously expressed its concern about the introduction of the notion of a lighter data protection regime for pseudonymised data. While pseudonymisation can represent an important safeguard with regard to for example data security, the use of pseudonymous or pseudonymised data is, in itself, not sufficient to justify a lighter regime on accountability obligations.[13]

The Working Party therefore would welcome a clear statement from the European Commission that under the current Directive further processing of mHealth personal data (even if pseudonymised) for historical, statistical and scientific research purposes generally requires the explicit consent of the data subjects, with exceptions as laid down in national law. In the future General Data Protection Regulation, the further processing of health data should only be permitted after having obtained the explicit consent of the data subjects, or if the narrow exceptions defined by the European Parliament apply. Any proposals to weaken and thereby broaden the scope of this type of further processing, such as a proposal to delete the word 'research', or proposals to remove both the consent and the opt-out requirement, should be negatively assessed in view of the real risks for data subjects of unequal/unfair treatment, based on the further processing, for example through profiling, of intimate data concerning their private life.

---

[13] See also Article 29 Working Party, WP 216, Opinion 05/2014 on Anonymisation Techniques, p. 10.
"A specific pitfall is to consider pseudonymised data to be equivalent to anonymised data. The Technical Analysis section will explain that pseudonymised data cannot be equated to anonymised information as they continue to allow an individual data subject to be singled out and linkable across different data sets. Pseudonymity is likely to allow for identifiability, and therefore stays inside the scope of the legal regime of data protection. This is especially relevant in the context of scientific, statistical or historical research."