A deep dive into dynamic data flows, wearable devices, and the concept of health data

Anni-Maria Taka*

Key Points

- Quantified Self Devices process data relating to the user's well-being and lifestyle, such as body temperature, heart rate, and physical exercise. These datasets are typically combined, generating, for example, observations and recommendations about various aspects of the user's well-being.
- As the data may relate to the user's health, the question is whether such data are considered health data under the General Data Protection Regulation (GDPR).
- Under the GDPR, data concerning health cover all personal data that relate to the physical or mental health of an individual. According to the list of examples provided in GDPR's recital, the concept of health data covers, *inter alia*, any information on disease risk or physiological state.
- It is, however, unclear whether, or to what extent, the concept of health data covers lifestyle and well-being data. This article examines the different components of the concept and analyses whether lifestyle and well-being data fall within the scope of the concept.
- This article suggests a four-step model, a health data assessment, to assess whether lifestyle and well-being data processed in connection with the use of Quantified Self Devices are health data. The health data assessment considers the content of the datasets, the context and purpose of the processing, and the usage of the data flows as well as the effects of the processing.

Introduction

Wearable devices, well-being, and data

Smart rings, watches, and other wearable devices for health and well-being are undoubtedly amongst the booming trends of our time. These devices and apps—also known as Quantified Self Things—enable users to monitor their daily habits and lifestyles. For the purposes of this article, such devices and apps are collectively referred to as 'Quantified Self Devices' or simply 'devices'. The data that are processed in connection with the use of the devices may include the user's body temperature, heart rate, steps, exercises, food consumption, mood, weight, and height.[1] The data may be provided by the user or perhaps measured or inferred by the device or the company that provides the device as part of its service (the 'service provider'). Data may also be provided by third parties, such as other app providers, if the data are disclosed between different apps. Depending on the device and its functionalities, it may also provide recommendations to the user, for example, to encourage the user to go to bed earlier or be more active. Some devices may also present overviews, such as figures or trends, showing how the user's body temperature has evolved during a certain period of time or

*Anni-Maria Taka, Faculty of Law, University of Helsinki, Helsinki, Finland

[1] Article 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (WP 223, 16 September 2014) 5; Article 29 Working Party, 'Annex – Health Data in Apps and Devices' (Letter to Paul Timmers, Director of Sustainable and Secure Society Directorate at the European Commission, 2015) <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> accessed 19 January 2022. The document is an annex to the letter from the Article 29 Working Party to the European Commission sent by Isabelle Falque-Pierrotin (Chairwoman) on behalf of the Article 29 Working Party on 5 February 2015 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf> accessed 7 January 2022. As a response to the European Commission's request, Article 29 Working Party clarifies, in the Annex, the scope of the definition of data concerning health in the context of lifestyle and well-being apps and devices; European Data Protection Supervisor, 'Opinion 1/2015 Mobile Health - Reconciling Technological Innovation with Data Protection' (21 May 2015) 3 and 10. See also Dominik Leibenger and others, 'Privacy Challenges in the Qualified Self Movement - An EU Perspective, in Proceedings on Privacy Enhancing Technologies' (2016) (4) De Gruyter Open Access Journals 315.

general observations about recovery.[2] As the devices are typically intended to be used on a regular basis, the users may monitor their lifestyle and well-being and observe any changes, trends, or developments.[3] Thus, the sensor data and combination of datasets may disclose insightful characteristics about the user's daily habits and preferences as well as their behaviour.[4]

Quantified Self Devices are part of the so-called 'Internet of Things' (IoT). IoT devices are also known as Smart Things or smart devices.[5] The WP29 has described the IoT in the following manner: 'The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.'[6] The WP29 has noted Quantified Self Things as one of the developments in the IoT that comes with privacy issues. Other categories of IoT include, for instance, Wearable Computing (such as watches, glasses, and other everyday objects equipped with sensors) and Domotics (home automation such as smart light bulbs and washing machines with remote controls). The line between these different IoT categories may be vague or they may overlap: for example, a wearable device, such as a smartwatch, maybe a Wearable Computing but also a Quantified Self Device.[7]

Research topic and methodological approach

This article analyses the nature of the data processed by Quantified Self Devices (or the service providers) in the light of the European Union's (EU) General Data Protection Regulation (GDPR) and its data categorization.[8] The focus of this analysis is on the data on the user's well-being and lifestyle. The GDPR does not recognize or define well-being data (nor lifestyle data), but these types of data may be considered health data. Thus, the starting point of the analysis is the GDPR's definition for data concerning health. According to the definition in Article 4(15) of the GDPR, data concerning health mean 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.

This article examines the following questions: Are data about well-being or lifestyle, processed in connection with the use of Quantified Self Devices, considered data concerning health under the GDPR? How is the nature of the data defined when any personal data have the potential to become health data at some point during its lifecycle? As a response to these questions, this article provides a legal analysis and a structured health data assessment, which is folded into a four-step model. This health data assessment consists of the following components: (i) content, (ii) context and purpose, (iii) usage, and (iv) effect. To construct the four-step model, this article identifies the main pillars and ingredients of health data as a concept, after which it presents the health data assessment.

As this article analyses applicable data protection legislation, and more precisely the provisions of the GDPR, it is natural to deploy the legal dogmatic method.[9] This article focuses on determining 'what the law is', instead of 'what the law ought to be', even though these two aspects (also known as lex lata and lege de ferenda) may not always be easily distinguished in the context of data protection legislation.[10] The analysis and the four-step model are based on various legal sources, such as the relevant case law of the Court of Justice of the European Union (CJEU or 'the Court'), guidelines and opinions from the

[2] These observations are based on my personal user experience of the wearable smart ring called Oura Ring, provided by the Finnish health technology company Oura Health Oy <https://ouraring.com/en> accessed 7 June 2022.

[3] Article 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 1) 5.

[4] Ibid 8; European Data Protection Supervisor, 'Opinion 1/2015 Mobile Health - Reconciling Technological Innovation with Data Protection' (21 May 2015) 10.

[5] Article 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 1) 4–6; Jenna Mäkinen, 'Data Quality, Sensitive Data and Joint Controllership as Examples of Grey Areas in the Existing Data Protection Framework for the Internet of Things' (2015) 24(3) Information & Communications Technology Law 262, 265–267; Jenna Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2017) International Journal of Law and Information Technology 1, 3; See also Stanislaw Piasecki and Jiahong Chen, 'Computing with the GDPR When Vulnerable People Use Smart Devices' (2022) 12(2) International Data Privacy Law 113, 116. For IoT, it is also relevant, *inter alia*, to consider the possible risks related to the use of the IoT in light of EU's proposal for the AI Act and assess whether and/or to what extent the requirements of the proposed AI Act are applicable. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final.

[6] Article 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 1) 4.

[7] Ibid 5–6.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[9] Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International, The Hague, The Netherlands 2002) 15.

[10] Ibid 16.

European Data Protection Board (EDPB) and its predecessor, the Article 29 Working Party (WP29), as well as academic literature about the concepts of health data and personal data in the GDPR. The core conclusions and remarks of this analysis are mostly influenced by the GDPR's recitals relating to data concerning health, the relevant CJEU case law regarding the concepts of health data and personal data (analysed in 'Health data as a concept' and 'Health data by nature and data flows that transfer into health data' sections), the EDPB's guidelines on the processing of data concerning health for the purpose of scientific research in the context of the Covid-19 outbreak, the WP29's opinion on the concept of personal data, and the WP29's 'Annex – Health Data in Apps and Devices'.[11]

While recitals are not legally binding, they provide valuable explanations for the interpretation of EU legislation.[12] The same applies to the EDPB's and the WP29's guidance, meaning that they do not have legally binding status, but they are, nevertheless, important and relevant for the interpretation of the GDPR's provisions.[13] Even though the CJEU does not always agree with the WP29's reasoning, CJEU case law shows that the WP29's interpretations (now the EDPB) may very well end up in the CJEU's own reasoning.[14] In *Nowak*, the Court repeated the idea of the WP29's three-step model (content, purpose, and result) for personal data by stating that information 'relates' to the data subject 'where the information, by reason of its content, purpose or effect, is linked to a particular person'.[15] The Court has also taken a stance on the definition of health data. As the CJEU has the final say on the interpretation of EU law, and thus on the concept of health data, it is important to acknowledge how the Court typically interprets EU legislation. In addition to the wording of the legal provision, the Court considers its context as well as the objectives of the legislation that the provision is part of.[16]

The CJEU, the EDPB, the WP29, academics, and other professionals have provided valuable analysis and guidance for determining what exactly constitutes health data and for solving the issue of the so-called grey areas.[17] Wearable devices that measure health and well-being are a relatively new phenomenon and the use of such devices raises complex data protection questions—one of them being the nature of data—that should be subject to further academic research. Having observed that there is room and need for further research in this field of law, this article seeks to provide fresh insights and further clarity on the issue of data categorization in the context of Quantified Self Devices.

It is important to know whether the data are health data as the nature of the data impacts the rights and requirements set forth in the GDPR, because certain special categories are treated differently from other types of personal data. Among other things, it influences the data subject's informational self-determination and level of control over his or her personal data, as well as the applicable legal ground(s) and requirements for the data processing. The fact that certain data fall within one of the special categories of personal data impacts the application of several provisions of the GDPR. To give some concrete examples, the nature of processing (such as the processing of special category data) must be taken into account when implementing data protection by design and default requirements, choosing appropriate technical and organisational measures and assessing the need for a data processing impact assessment, just to mention a few concerns.[18]

[11] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2007); Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1); European Data Protection Board, 'Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak' (21 April 2020).

[12] *Mowi ASA v European Commission*, Case C-10/18 P, [2020] (ECLI:EU:C:2020:149) para 44; *Hungary v Parliament and Council*, Case C-156/21, [2021] (ECLI:EU:C:2021:974) paras 191 and 332; *Vyriausioji tarnybinès etikos komisija*, Case C-184/20, [2022] (ECLI:EU_C:2022:601) para 124. See also European Commission, Legal service, 'Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union legislation' (2016) Publications Office, 31 <https://op.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732> accessed 7 July 2022; Rosemary Jay, *Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice* (1st edn, Sweet & Maxwell, London 2017) 49–50.

[13] GDPR, Art 70; Jay Ibid 25; Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40, 43, 59.

[14] Purtova (n 13) 59–60, 70. Purtova refers to *Peter Nowak*, Case C-434/16, [2017] (ECLI:EU:C:2017:994).

[15] *Peter Nowak*, Case C-434/16, [2017] (ECLI:EU:C:2017:994) para 34–35; Purtova (n 13) 70.

[16] *Bank Melli Iran*, Case C-124/20, [2021] (ECLI:EU:C:2021:1035) para 43; *Vyriausioji tarnybinès etikos komisija*, Case C-184/20, [2022] (ECLI:EU:C:2022:601) para 121. See also Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' 2019(2) Columbia Business Law Review 494, 533.

[17] For eg, Malgieri and Comandé suggest an approach that focuses on two indicators, namely 'intrinsic sensitiveness' of the data and 'computational distance' between the dataset and sensitive (health) data, see Gianclaudio Malgieri and Giovanni Comandé, 'Sensitive-by-Distance: Quasi-health Data in the Algorithmic Era' (2017) 26(3) Information & Communications Technology Law 229, 238. Schäfke-Zell proposes a method of seven steps to assess whether data are health data, focusing on linkability and inferability, see Werner Schäfke-Zell, 'Revisiting the Definition of Health Data in the Age of Digitalized Health Care' (2021) International Data Privacy Law 10.

[18] GDPR, arts 9, 25, 32, and 35. See also Article 29 Working Party, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (version 2.0, 20 October 2020) 9.

This article is structured in the following manner: 'Relevant legal framework' section introduces the relevant legal framework applicable to the processing of health data in the EU. 'Health data as a concept' section unfolds the concept of health data and identifies the three pillars on which the concept stands. 'Health data by nature and data flows that transfer into health data' section focuses on the various forms of health data and how personal data may transform into health data. 'Four-step health data assessment' section suggests a four-step model to assess whether personal data are considered health data under the GDPR. Finally, the last section presents the concluding remarks.

Relevant legal framework

The GDPR and special categories of personal data

Typically, the data collected and processed in connection with the use of Quantified Self Devices are personal data. The GDPR regulates the processing of personal data in the EU and, to some extent, even outside EU territory.[19] The GDPR treats certain types of datasets, namely datasets that belong to the special categories of personal data, with special care due to their sensitive nature.[20] As noted by the CJEU, due to the 'particular sensitivity' of the data, the processing of such data is 'liable to constitute, as also follows from recital 33 of [Directive 95/46] and recital 51 of [the GDPR], a particularly serious interference with the fundamental rights to privacy and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter.'[21] Such data are considered to fall within the inner circle of our privacy and within the most intimate and vulnerable area of our existence.[22] Processing of sensitive data may result in high risks to the fundamental rights and freedoms of a data subject because sensitive conclusions can be drawn based on such data.[23] Further, the reason behind the special treatment of certain data categories is the negative and harmful consequences that any misuse of such data may have for data subjects.[24] Thus, the processing of sensitive data is subject to higher standards compared to other types of personal data. The special categories of personal data are listed in Article 9 of the GDPR, and the data concerning health are one of the categories that enjoy special protection.[25] For the purposes of this article, data concerning health are also referred to as 'health data'.

The main rule in Article 9 of the GDPR is that the processing of special categories of personal data is forbidden. Processing of such data may take place only if at least one of the derogations listed in Article 9(2) applies. For example, health data may be processed if the processing is based on the data subject's explicit consent, or if the processing is necessary for the purposes of medical diagnosis, treatment, public interest, or scientific research on the basis of EU or Member State law. In addition to the derogations in Article 9, any processing of health data must also have a legal basis in Article 6 to be considered lawful.[26] As noted by the WP29, the placement and retrieval of any personal data in connection with an app installation requires, in principle, the app user's consent, in accordance with the ePrivacy Directive. However, once the app is installed and the user starts using it, later processing of personal data during the use of the app may be based on the data subject's consent or another legal ground.[27] If the data that are processed during the use of the app or the device are special category data, then the situation is more complex, as the processing must have an applicable ground in Article 9 as well.[28] To sum up, any processing of health data in connection with the use of a Quantified Self Device requires valid consent when the app is installed as well as an applicable legal basis (Article 6) together with a suitable derogation (Article

[19] Regarding GDPR's territorial scope, see GDPR, Art 3.

[20] See GDPR, Art 9 and recital 51.

[21] *GC and Others* (De-referencing of sensitive data*)*, Case C-136/17, [2019] (ECLI:EU:C:2019:773) para 44.

[22] Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) Council of Europe Treaty Series 223, ch II, Art 6 (para 55); Lee A Bygrave and Luca Tosoni, 'Article 4(15). Data Concerning Health' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (OUP, Oxford, UK 2020) 218.

[23] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing, Cham, Switzerland 2017) 110.

[24] Article 29 Working Party, 'Advice Paper on Special Categories Of data ("sensitive data")' (20 April 2011) 4.

[25] According to GDPR, Art 9, the following categories are considered special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. See also GDPR, recital 53.

[26] This was confirmed by European Data Protection Board in European Data Protection Board (n 11) 6.

[27] Article 29 Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (WP 202, 27 February 2013) 14 and 16. WP29 refers to the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), the 'ePrivacy Directive'. Article 5(3) of the ePrivacy Directive states, among other things, that the subscriber must be provided with clear and comprehensive information in accordance with Directive 95/46/EC (repealed by the GDPR).

[28] Ibid 16; European Data Protection Board (n 11) 6.

9) for the entire use of the app or the device and as long as the data are processed. However, the possible legal bases for the processing do not fall within the scope of this article and are not subject to further analysis.

At this point, it is important to note that this article examines devices that are typically not designed for medical purposes and are, therefore, not considered medical devices under the Medical Devices Regulation (MDR).[29] Instead, the focus is on devices that are used by consumers and regulated by consumer protection legislation. The devices may also be purchased by an employee and the contractual relationship may, in such cases, be between the service provider and the employer, the employees being the users of the devices.[30] However, these contractual and consumer protection aspects are not further discussed in this article, as they should not, in my understanding, affect the analysis relating to the research questions.[31]

Nature of the Qualified Self Device and its intended use

In the EU, medical devices are regulated by the MDR. According to recital 19 of the MDR, software that is 'specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device, while software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device'. Thus, the intended purpose, which means 'the use for which a device is intended' and which is determined by the manufacturer of the device, is decisive.[32] This article looks at devices that are intended for lifestyle and well-being purposes and not for medical purposes. The European Commission has noted that no binding rules exist for determining the borderline between lifestyle and well-being apps on the one hand, and medical devices or in vitro diagnostic medical devices on the other.[33]

Lifestyle and well-being devices may not be medical devices, but most of them are 'intended to directly or indirectly maintain or improve healthy behaviours, quality of life and well-being of individuals'.[34] Typically, these devices provide data about the user's daily activities and sleep, so that the users can monitor their lifestyle and well-being. The purpose of the device is in general revealed in the service provider's terms and conditions where the service is defined, whereas the purpose of the data processing is introduced in the service provider's privacy policy. For example, Fitbit explains in its Terms of Service that it 'designs products and tools that help [users] achieve [their] health and fitness goals and empower and inspire [users] to lead a healthier, more active life'.[35] Further, Fitbit's privacy policy states that the company processes personal data for, among other things, the provision and maintenance of the service (which is described in the Terms of Service).[36] This example shows that the purpose of the service, including the intended use of the device, has a direct influence on the purpose of use of the data. A third aspect is the purpose for which the user/consumer uses the device. Users may, for example, want to use the device 24/7 to monitor their sleep, activities, and recovery, in order to have a better understanding of not only their well-being but also their health. Other users may perhaps want to focus on tracking certain activities and steps taken and use it only while exercising. Different devices provide different functionalities: some devices focus on monitoring sleep, while others may provide more specific data for exercising. All in all, the intended purpose determined by the manufacturer, the user's own purpose of use of the device, as well as the purpose of data processing are in a dynamic relationship with each other, and they all influence the data processing, that is what data are processed, how they are processed, and so on.

Qualified Self Devices lack proper regulatory status, as they fall between medical products and traditional consumer products. The currently applicable EU legal framework in the field of health care does not explicitly recognise these lifestyle devices as there is no category under which such devices would fall.[37] It should be

[29] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ 2017 L 117/1.

[30] Regarding wearable devices in an employment context, see Céline Brassart Olsen, 'To Track or Not to Track? Employees' Data Privacy in the Age of Corporate Wellness, Mobile Health, and GDPR' (2020) 10(3) International Data Privacy Law 236.

[31] Regarding consumer protection aspects associated with tracking apps, see eg Anastasia Siapka and Elisabetta Biasin, 'Bleeding Data: The Case of Fertility and Menstruation Tracking Apps' 2021 10(4) Internet Policy Review 1.

[32] MDR, Art 2(12).

[33] European Commission, 'Green Paper on mobile Health ("mHealth")' COM (2014) 219 final, 11.

[34] Ibid 3 (footnote 2).

[35] Fitbit's Terms of Service (31 July 2021) < https://www.fitbit.com/global/us/legal/terms-of-service> accessed 20 January 2022.

[36] Fitbit's Privacy Policy (16 August 2021) <https://www.fitbit.com/global/us/legal/privacy-policy#how-we-use-info> accessed 27 January 2022.

[37] Federica Lucivero and Barbara Prainsack 'The Lifestylisation of Healthcare? 'Consumer Genomics' and Mobile Health as Technologies for Healthy Lifestyle' (2015) 4 Applied & Translational Genomics 44, 45, 47.

noted, however, that the criteria set forth for the processing of health data in the GDPR does not require that the device is a medical device.[38] In other words, the device may process health data regardless of whether it is a medical device under the MDR. Thus, the nature of the device is not a decisive factor in assessing the nature of the data.

Health data as a concept

Familiar concept with a novel definition

The concept of health data is not a new phenomenon in European or international instruments. It is present, for example, in the Data Protection Directive that precedes the GDPR, as well as in the Council of Europe's Convention 108 and the Modernised Convention 108.[39] Even so, these instruments do not actually define the concept. Having said that, the Explanatory Report to the Convention 108 from 1981 (here 'Report 1981') explains that personal data concerning health include information about an individual's physical as well as mental health (past, present, and future). The concept covers information relating to healthy, sick, and deceased persons. Interestingly, Report 1981 mentions that personal data concerning health also refer to data concerning 'abuse of alcohol or the taking of drugs'.[40] However, the Explanatory Report to the Modernised Convention 108 (here 'Report 2018') does not mention alcohol abuse nor the use of drugs. Report 2018 explains, *inter alia*, that '[i]nformation concerning health includes information concerning the past, present and future, physical or mental health of an individual, and which may refer to a person who is sick or healthy'.[41] As with the GDPR, data relating to deceased persons are not covered by the Modernised Convention 108.[42] Report 2018 also states that images that include health-related aspects (eg a broken leg or thick glasses) are considered sensitive data only if 'the processing is based on the health information that can be extracted from the pictures'.[43] A similar approach is taken by the EDPB in its guidelines relating to video devices. The EDPB argues that if a person wears glasses on a piece of video footage, then this is not automatically considered health data. Nevertheless, the requirements for health data are met 'if the video footage is processed to deduce special categories of data', for example if a hospital has installed a video camera for monitoring purposes.[44]

The GDPR's definition of health data bears many similarities with the two Explanatory Reports. The concept of health data is explained in recital 35 of the GDPR, according to which it covers all personal data 'pertaining to the health status of a data subject which reveal information relating to the past, current, or future physical or mental health status of the data subject'. Recital 35 provides the following examples of data concerning health:

- information collected in the course of registration for, or the provision of healthcare services;
- number, symbol, or particular assigned to a natural person to uniquely identify the natural person for health purposes;
- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and
- any information on a disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical state of the data subject.

Again, it should be borne in mind that the recitals of the GDPR are not legally binding, which means that the list of examples provided in recital 35 has no legally binding status either. Nevertheless, the recitals may very well provide valuable insights and illustrative guidance in interpreting the concept of health data.

The CJEU's approach to the concept of health data

The concept of health data has a wide scope, covering a large range of data. The Court stated in *Lindqvist* that data concerning health 'must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an

[38] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 2.

[39] EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108; Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018. Different instruments use, to some extent, different terms for health-related data, see Trix Mulder, 'The Protection of Data Concerning Health in Europe' (2019) 5 European Data Protection Law Review 209.

[40] Council of Europe, 'Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (Strasbourg, 28 January 1981) European Treaty Series No 108, ch II, Art 6 (para 45).

[41] Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) Council of Europe Treaty Series No 223, ch II, Art 6 (para 60).

[42] Ibid ch I, Art 3 (para 30). See also GDPR, recital 27.

[43] Council of Europe (n 41) ch II, Art 6 (para 60).

[44] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (version 2.0, 29 January 2020) 17.

individual'. The health-related aspect of the case concerned a person who had injured her foot and was on half-time on medical grounds.[45] The wide interpretation has been confirmed, by reference to *Lindqvist*, in other judgments of the Court, for example in *CN*. However, in *CN*, the Court also mentioned that the notion of data concerning health cannot be 'extended to include expressions which do not give rise to the disclosure of any data regarding a person's health or medical condition' and referred to its previous case *Dionyssopoulou*.[46] In *Dionyssopoulou*, the Court concluded that 'personal constraints' do not fall within the definition of health data.[47]

In its recent case, *Vyriausioji tarnybinės etikos komisija*, from August 2022, the CJEU once again referred to Lindqvist and stated that the concept of health data should be given a wide interpretation.[48] This time, however, the Court did not refer to *Dionyssopoulou.* I argue that if the question raised in Lindqvist would, today, be analysed in light of the GDPR and its examples in recital 35, the fact that someone has injured her foot and is on half-time on medical grounds would undoubtedly be information about her physical state, and thus health data. Thus, it can be questioned whether a wide interpretation was meant to be deployed even in situations where the information has only an indirect link to the person's health.

The judgment in *Vyriausioji tarnybinės etikos komisija* was delivered by the Court's Grand Chamber, which underlines the significance of the case. The Court may decide to refer a case to the Grand Chamber when, *inter alia*, it finds that it is of exceptional importance.[49] In *Vyriausioji tarnybinės etikos komisija*, the CJEU examined whether the special categories of personal data in Article 8(1) of Directive 95/46 and Article (9) of the GDPR include 'personal data that are liable to disclose indirectly the political opinions, trade union membership or sexual orientation of a natural person'.[50] The case concerned the publication of personal data on the website of an authority that has the responsibility to collect and check the content of declarations of private interests. The Court answered in the affirmative, meaning that 'personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data, for the purpose of those provisions'.[51] Even though the judgment concerned data that are indirectly linked to a person's sex life, and not health, the Court explicitly analysed the concept of health data as well. This is because of the wording in Article 9(1) of the GDPR, according to which data 'concerning' (in French *concernant*) health or data 'concerning' sexual life or sexual orientation are prohibited. Further, Article 9(1) forbids the processing of personal data 'revealing' (in French '*révèle*') racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person.[52]

Should the special categories of personal data be interpreted differently depending on the special category in question (and whether the wording is 'concerning' or 'revealing')? According to the opinion of Advocate General Pikamäe, the answer is no, as the approach to the processing of sensitive data should not vary according to the type of special category data in question. Advocate General Pikamäe noted that 'the word "concerning" strikes a more direct and immediate link between the processing and the data concerned', while using the verb 'reveal', on the other hand, is 'consistent with the taking into account of processing that not only is of inherently sensitive data but indirectly enables disclosure thereof following an intellectual exercise involving deduction or cross-referencing'.[53] The Advocate General's interpretation was supported by the CJEU and referred to in the CJEU's reasoning.[54] Furthermore, the Court noted that the word 'reveal' is used in recital 35 of the GDPR, as the recital explains that health data consist of personal data pertaining to the health status of a data subject which 'reveals' information relating to the past, current, or future physical or mental health status of the data subject.[55] The conclusion that can be made here is that, according to the Court, personal data 'concerning' health should be interpreted broadly, meaning that any personal data that 'reveal' the health status of the natural person should be considered health data.

The Court did confirm, in *Vyriausioji tarnybinės etikos komisija*, that indirect information about a person's health should be considered health data. In light of the

[45] Bodil Lindqvist, Case C-101/01, [2003] ECR I-12971 (ECLI:EU:C:2003:596), paras 49 and 50. See also Bygrave and Tosoni (n 22) 221–222.

[46] *CN*, Case T-343/13, [2015] (ECLI:EU:T:2015:926) para 50.

[47] *Triantafyllia Dionyssopoulou*, Case T-105/03 (ECLI:EU:T:2005:189) para 33. See also Bygrave and Tosoni (n 22) 221.

[48] *Vyriausioji tarnybinės etikos komisija*, Case C-184/20, [2022] (ECLI:EU:C:2022:601) para 125. See also eg, Case *CN* (n 46) para 50.

[49] Consolidated Version of the Statute of the Court of Justice of the European Union [2012] OJ 326/213 Art 16(5).

[50] Case *Vyriausioji tarnybinės etikos komisija* (n 48) para 117.

[51] Ibid para 128.

[52] Ibid paras 122–124.

[53] *Vyriausioji tarnybinės etikos komisija*, Case C-184/20, [2022] (ECLI:EU:C:2022:601), Opinion of AG Pikamäe, para 85.

[54] Case *Vyriausioji tarnybinės etikos komisija* (n 48) paras 123–124.

[55] Ibid para 124.

Court's reasoning, if the data are capable of revealing the health status of the natural person 'by means of an intellectual operation involving comparison or deduction', then the data should be considered health data.[56] However, what this means, de facto, in the context of Quantified Self Devices, is unclear and needs to be further analysed in the following sections.

Finally, it should be briefly noted that the confidentiality of health data also appears in the cases of the European Court of Human Rights (ECtHR) relating to, *inter alia*, the right to respect for private life under Article 8 of the European Convention on Human Rights, the leading judgment being *Z v Finland*. The health-related aspect in these cases concerned medical data, and the ECtHR underlined the importance of the confidentiality of health data, describing it as a 'vital principle'.[57] The CJEU's argumentation in *Vyriausioji tarnybinės etikos komisija* and *Lindqvist* regarding the wide interpretation of the concept of health data is, to some extent, similar to the ECtHR's reasoning in its case law. In *Vyriausioji tarnybinės etikos komisija*, the CJEU noted the following: 'Furthermore, a wide interpretation of the terms "special categories of personal data" and "sensitive data" is confirmed by the objective of Directive 95/46 and the GDPR, noted in paragraph 61 of the present judgment, which is to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular of their private life, with respect to the processing of personal data concerning them (. . .)'.[58] Both the CJEU and the ECtHR highlight the significance of the confidentiality of health data, which deserves a high level of protection.[59] Also, both the CJEU and the ECtHR consider the risks or negative consequences that the processing of health data may have for the individual.[60]

Are all personal data considered health data?

Even though the concept of health data is not a novel notion, the actual scope of it is far from clear or predictable. The European Data Protection Supervisor (EDPS) has stated that, '[i]n the absence of a clear definition, after an assessment of the case-specific circumstances, [the concept] should be construed broadly (. . .)'.[61] The WP29, which has provided several guidelines and opinions about EU's data protection legislation, has itself acknowledged that '(...) due to the wide range of personal data that may fall into the category of health-related data, this category represents one of the most complex areas of sensitive data and one where the Member States display a great deal of legal uncertainty'.[62] Thus, it is crucial to come up with methods and guidance so that health data receive special protection in accordance with the GDPR.

The WP29 has recognised a grey area that consists of complex cases where it is unclear whether the data should be considered health data. These datasets refer indirectly to health and indirectly reveal information about an individual's health status.[63] The legal status of this grey area is, however, still an unsolved and hotly debated topic.[64] Some legal scholars have even suggested that these types of data could form a separate data category of quasi-health data.[65] However, it is not clear that this would solve the problem with unclear notions. The question would then be whether certain data are health data, quasi-health data, or other personal data. Instead of two unclear concepts, there would be three.

Other legal scholars have argued that the classification of data into special categories is 'no longer meaningful'[66], and that it is increasingly challenging to determine whether certain datasets are sensitive.[67] Due to the context-dependent nature of health data, any personal data have the potential to be health data.[68] Indeed, the concept of health data is dynamic and may change over time, as its health-related nature is influenced by the circumstances of the processing, including technological

[56] *Vyriausioji tarnybinės etikos komisija* (n 48) para 120.

[57] European Convention for the Protection of Human Rights and Fundamental Freedoms, 3 September 1953, ETS 5, 213 UNTS 221, Art 8; *Z v Finland* (1997) ECtHR 1997-I, para 95; *MS v Sweden* (1997) ECtHR 1997-IV, para 41; *Kotilainen and Others v Finland* App no 62439/12 (ECtHR, 17 September 2020) para 83; *YG v Russia* App no 8647/12 (ECtHR, 30 August 2022) para 44; *MK v Ukraine* App no 24867/13 (ECtHR 15 September 2022) para 34; See also Bygrave and Tosoni (n 22) 221.

[58] Case *Vyriausioji tarnybinės etikos komisija* (n 48) para 125. The CJEU further refers to the Case *Lindqvist* (n 45) para 50. See also Bygrave and Tosoni (n 22) 221–222.

[59] Ibid.

[60] Case *Vyriausioji tarnybinės etikos komisija* (n 48) para 126; *Z v Finland* (n 57) paras 95–96.

[61] European Data Protection Supervisor (n 1) 6.

[62] Article 29 Data Protection Working Party (n 24) 10. Article 29 Working Party uses the term 'health data' instead of 'data concerning health'.

[63] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 3. See also Malgieri and Comandé (n 17) 229, 235.

[64] See eg, Malgieri and Comandé (n 17) 229, 244.

[65] Ibid 235–236.

[66] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (25 May 2016) 11 <https://ssrn.com/abstract=2784123> accessed 7 June 2022.

[67] Ibid; Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 995, 1014.

[68] See Moerel and Prins (n 66) 56–57. See also W Kuan Hon, Christopher Millard and Ian Walden, 'The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated? - The Cloud of Unknowing' (2011) 1(4) International Data Privacy Law 211, 225.

capabilities.[69] According to legal scholars, one way forward could be a risk-based approach instead of categorisation.[70] Another approach is to consider the sensitiveness of the use of the data.[71] On the other hand, data categorisation has a 'symbolic value', as it underlines that certain data needs special protection because the processing of such data may 'generate substantial harm'.[72]

While I do acknowledge these problematic aspects, the special categories reflect the GDPR's aim to provide special protection to the most sensitive data types. Further, the categorisation is not, per se, an obstacle to a contextual or risk-based approach. Nevertheless, the value of dividing datasets into different categories depends on how the special categories are interpreted. If a very broad interpretation is the way forward, meaning that in principle any personal data are health data, the data categorisation will indeed lose its relevance. On the other hand, if the concept stands firmly on clear and structured components, enabling health data assessment, the data categorisation may well remain significant in the future. This article takes the latter approach and seeks to provide an understandable model to tackle the problematic issue of health data.

The concept stands on three pillars

In the GDPR, the concept of health data is built on three components: (i) personal data; (ii) concerning; and (iii) health. First, only personal data can be considered data concerning health. Secondly, the data must 'concern' health. Thirdly, the data must relate to the 'health' of the individual. In other words, the concept is about personal data and health, and about a certain connection between them.

The first component is 'personal data'. To be considered health data, the data in question must meet the criteria set forth for the notion of personal data. Personal data mean any information relating to an identified or identifiable natural person ('data subject').[73] The WP29 perceives the concept as a combination of four main building blocks, namely: (i) any information; (ii) relating to; (iii) an identified or identifiable; and (iv) natural person.[74] Each of these must be addressed when examining whether a certain dataset is personal data.

Generally, the criterion of personal data is fulfilled when data are collected by means of a Quantified Self Device, but there may, of course, be situations where this is not the case.[75] For the purposes of this article, the criteria for personal data must be met, but these requirements are not analysed in further detail in this article. However, the notion has a broad scope and, as noted by Purtova, '(...) European data protection law is facing a risk of becoming "the law of everything", meant to deliver the highest legal protection under all circumstances, but in practice impossible to comply with and hence ignored or discredited as conducive to abuse of rights and unreasonable'.[76] The concept of health data may face the same risks if interpreted too broadly. Regarding inferences, Wachter and Mittelstadt have noted that it is unclear whether they are considered personal data and what rights data subjects have in relation to inferences.[77]

The second component is 'concerning'. The personal data must be 'relating to' the health status, as expressed in recital 35 of the GDPR. The WP29 has stated that the processing of personal data relates to a person's health when the data have 'a clear and close link with the description of the health status of a person'.[78] However, the CJEU's recent interpretation in *Vyriausioji tarnybinės etikos komisija* shows that this interpretation cannot be adopted in relation to special categories of personal data (see 'The CJEU's approach to the concept of health data' section).

The expression 'relating to' is also used in the definition of personal data, in Article 4(1) of the GDPR, as personal data mean any information relating to an identified or identifiable natural person. Further, recital 26 explaining the concept of personal data states that the principles of data protection should apply to 'any information concerning' an identified or identifiable natural person.

The WP29 has provided guidance about the component 'relating to' in the definition of personal data, as it has explained that one of the three elements—namely content, purpose, or result—must be met.[79] As noted in the introduction of this article, these three elements were also acknowledged by the Court in *Nowak*, as the Court stated that information 'relates' to a data subject

[69] Malgieri and Comandé (n 17) 248.

[70] Hon, Millard and Walden (n 68) 225–226.

[71] Moerel and Prins (n 66) 11.

[72] Zarsky (n 67) 1013–1014.

[73] GDPR, Art 4(1).

[74] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11) 6. See also Purtova (n 13) 45–59.

[75] European Data Protection Supervisor (n 1) 4–5.

[76] Purtova (n 13) 41.

[77] Wachter and Mittelstadt (n 16) 498.

[78] Article 29 Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)' (WP 131, 15 February 2007) 7.

[79] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11) 9–12. See also Lee A Bygrave and Luca Tosoni, 'Article 4(1). Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (OUP, Oxford, UK 2020) 110.

if it is linked to a certain individual due to its content, purpose or effect.[80] In *Nowak*, the CJEU concluded that the written answers of a candidate at a professional examination are considered personal data in those circumstances.[81] Interestingly, the Court used the wording 'effect' instead of 'result' (which is used by the WP29).

According to the WP29, the content element exists in cases where data are clearly about an individual, such as a diagnosis that clearly relates to a certain patient. As to the purpose element, it is present in situations where the data are used, or is likely to be used to evaluate, influence, or treat a person in a certain way. Finally, the result element refers to cases where the use of data is likely to have an impact (major or not) on an individual's rights and interests, for example that the individual may be treated differently due to the data processing activities. For the evaluation of both the purpose element and the result element, the circumstances in each individual case are relevant.[82]

The third component is 'health'. According to the World Health Organization's (WHO) definition, health is 'a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity'.[83] The WHO has, however, noted that their definition portrays an ideal and that all health development activities should perceive it as a goal.[84] Many factors influence health, including medical but also social factors, such as education, income, and working conditions.[85] Economic, psychological, and environmental circumstances may also influence one's health.[86] Thus, the WHO's approach to health is very broad, covering in principle all aspects of life. It is also important to understand that the WHO's objective is 'the attainment by all peoples of the highest possible level of health', as stated in Article 1 of the Constitution of the WHO. In light of this objective, it is understandable that the concept of health has a wide scope. As argued in the following sections of this article, such a wide approach to health in the GDPR's definition of health data would be neither convenient nor desirable. While it is important to be aware of the WHO's definition of health, the concept of health data should be interpreted, in each individual case, in light of the GDPR's purposes and the context of the data processing.

Further, the relationship between health and well-being is particularly interesting in the context of Quantified Self Devices, as the data is about well-being and lifestyle. WHO has noted that well-being is an integral part of its definition of health. Well-being consists of both subjective (such as person's sense of well-being) and objective aspects (such as health, education, and social relationships).[87]

The European Commission has also indicated that health and well-being are not synonyms, even though they may overlap. For example, the Communication document provided by the European Commission regarding the eHealth Action Plan 2012–2020 ('Communication') distinguishes between health and well-being data, which is pointed out by EDPS in its opinion to the Communication.[88] Also, in its *Google/Fitbit* case, the European Commission mentions 'health and wellness data'[89] and 'health and fitness data',[90] and thus implies that lifestyle and well-being data are not the same thing as health data. However, it also notes that collection of health data, such as exercise data, lifestyle data, and data from health risk assessments, is possible under corporate wellness programmes.[91] Also, the EDPS has clarified that the category of well-being data may include personal data that relate to health.[92]

All in all, health and well-being seem to be two separate concepts that are closely linked to each other and,

[80] Case *Nowak* (n 15) para 34–35; Purtova (n 13) 70.

[81] Ibid para. 62. However, in the CJEU's joined cases C-141/12 and C-372/12, the CJEU analysed the nature of the data relating to an applicant for a residence permit and found that the legal analysis in a minute does not, in itself, constitute personal data. See *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Joined Cases C-141/12 and C-372/12, [2014] (ECLI:EU:C:2014:2081) para 39.

[82] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11) 10–11.

[83] Constitution of the World Health Organization 1946 (amended in 1977, 1984, 1994, and 2005).

[84] World Health Organization, 'Health21 - The Health for All Policy Framework for the WHO European Region' (European Health for All Series No 6) 3, 211 <https://www.euro.who.int/__data/assets/pdf_file/0010/98398/wa540ga199heeng.pdf> accessed 26 January 2022.

[85] World Health Organization's website 'Social Determinants of Health' <https://www.who.int/health-topics/social-determinants-of-health#tab=tab_1> accessed 26 January 2022.

[86] World Health Organization, Regional Office for Europe, 'Health2020: A European Policy Framework and Strategy for the 21st Century' (2013) 39 <https://www.euro.who.int/__data/assets/pdf_file/0011/199532/Health2020-Long.pdf> accessed 14 July 2022.

[87] Ibid 181.

[88] European Data Protection Supervisor, 'Opinion on the Communication from the Commission on "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century"' (27 March 2013) 3 (para 10) <https://edps.europa.eu/data-protection/our-work/publications/opinions/ehealth-action-plan-2012-2020_en> accessed 14 July 2022; European Commission, 'Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century' COM(2012) 736 final, ch 4.3 <https://health.ec.europa.eu/publications/ehealth-action-plan-2012-2020_en> accessed 19 August 2022.

[89] *Case M.9660 - Google/Fitbit*, Commission Decision of 17 December 2020 declaring a concentration to be compatible with the internal market and the EEA agreement, C (2020) 9105 final, para 272.

[90] Ibid para 484.

[91] Ibid para 483.

[92] European Data Protection Supervisor (n 88) 3 (para 10).

to some extent, overlap. However, the boundary between health and well-being—and similarly between health data and well-being data—is ambiguous. As the GDPR has no separate definition for well-being data, the relevant question is whether such data are health data or just casual personal data. Well-being data could also fall into other special categories of personal data, such as biometric data,[93] but those aspects are outside of the scope of this article.

Sensitive health data or just personal data?

Quantified Self Devices process different types of datasets relating to the user's lifestyle and well-being. Malgieri and Comandé approach the nature of the data in relation to health and lifestyle apps by dividing the data into raw data ('user-generated data') and complex data ('data controller generated data').[94] The WP29 has, in its guidance relating to automated decision making and profiling, taken a similar approach to different types of personal data in general. The WP29 recognises the following categories (list of examples): provided data, observed data, and derived or inferred data.[95] The same approach is taken in an article by Comandé and Schneider, noting that the categorisation is based on OECD's Report on Data-Driven Innovation for Growth and Well-being.[96] In Malgieri's and Comandé's article, raw data are further divided into received and observed data, and complex data into inferred data and predicted data. Received data refer to datasets provided by the user, such as information about diagnosis, mood, and weight. Observed data are data collected by sensors of the devices, for example heart rate, body temperature, and number of steps taken. Inferred and predicted data are based on the raw data or combinations of datasets. Inferred data reflect the past or present state of well-being, while predicted data focus on the future state of the user's well-being.[97] Wachter and Mittelstadt define inferences as personal data that are '(...) created through deduction or reasoning rather than mere observation or collection from the data subject'.[98]

The categorization—received data, observed data, inferred data, and predicted data—will also be used in this article. However, instead of raw data and complex data, this article refers to input data and output data as these, in my view, capture the essence of the data that transforms into health data: the data (input data) are provided to or measured by the device, after which the data are combined with other data or otherwise used in a way that generates new, health-related data (output data). These terms describe the changing nature of the data.[99] The big question remains, namely whether these different types of input and output data fall within the scope of the GDPR's definition of health data.

Most of the examples in recital 35 concern personal data that are health data either because the data itself is clearly health related (such as a disease or medical history) or because the processing takes place in a healthcare context and for medical purposes. However, the recital does not reveal whether, or to what extent, data about well-being and lifestyle are considered health data.[100] According to the recital, the concept of health data covers, *inter alia*, any information on disease risks and physiological state of the data subject, regardless of its source. How broadly should these examples be understood? Do lifestyle and well-being data fall within the scope of information on disease risks or physiological state, and thus health data? The wording 'any information' indicates the legislator's will for a broad scope, which was also noted by the Court in *Nowak* concerning the concept of personal data.[101]

As mentioned above, the examples listed in recital 35 are considered health data independent of their source. The EDPB has further clarified the concept by providing a list of examples concerning possible sources from which health data may be derived:

1. Information collected by a healthcare provider in a patient record (such as medical history and results of examinations and treatments).
2. Information that becomes health data by cross-referencing with other data thus revealing the state of health or health risks (such as the assumption that a person has a higher risk of suffering heart attacks based on the high blood pressure measured over a certain period of time).

[93] See Brassart Olsen (n 30) 244.

[94] Malgieri and Comandé (n 17) 232.

[95] Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679' (WP251rev.01, 3 October 2017, as last revised and adopted 6 February 2018) 8. See also Sandra Wachter and Brent Mittelstadt (n 16) 516.

[96] OECD, 'Report on Data-Driven Innovation for Growth and Well-being' (2014) 65 <https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf> accessed 12 July 2022; Giovanni Comandé and Giulia Schneider, 'Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of Health Data' (2018) 25 European Journal of Health Law 284, 292.

[97] Malgieri and Comandé (n 17) 232.

[98] Wachter and Mittelstadt (n 16) 515.

[99] These terms are used eg in Wachter and Mittelstadt (n 16) 514. See also Tuomas Pöysti, 'The IIoT and Design for Contextually Relevant Data Protection' in Rosa Maria Ballardini, Petri Kuoppamäki and Olli Pitkänen (eds), *Regulating Industrial Internet Through IPR, Data Protection and Competition Law* (Wolters Kluwer, AH Alphen aan den Rijn, The Netherlands 2019) 197.

[100] See European Data Protection Supervisor (n 1) 6.

[101] Case *Nowak* (n 15) para 34; Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11) 6. See also Purtova (n 13) 66.

3. Information from a 'self-check' survey, where data subjects answer questions related to their health (such as stating symptoms).
4. Information that becomes health data because of its usage in a specific context (such as information regarding a recent trip to or presence in a region affected with Covid-19 processed by a medical professional to make a diagnosis).[102]

These examples include similar elements to the summary provided by the WP29 in 2005 regarding lifestyle and well-being apps and devices, according to which 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 conclusions 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.[103]

The first category in the WP29's summary (above), namely data that are inherently/clearly medical data, is similar to the EDPB's example 1, as they both refer to clear cases of health data. As to the WP29's second category concerning combinations and conclusions, similar elements are present in the EDPB's example 2, while the WP29's third category is perhaps closest to the EDPB's examples 3 and 4.[104]

Health data by nature and data flows that transfer into health data

Health data in patient records

The EDPB's example 1 represents clear cases of health data, namely information in patient records, such as the patient's medication, previous or current diseases, symptoms, or blood test results, collected in a healthcare context. In these cases, the data source is a healthcare provider. These datasets are originally collected and processed for medical purposes, such as for medical diagnosis and medical treatment. The data remain health data even if they are further processed in another context or for secondary purposes (eg, for scientific research). Thus, the data continue to be health data even if they flow from a healthcare system to another system outside the healthcare context. For example, patients may want to receive their data from a healthcare provider via certain well-being applications or provide their well-being data from the application to the healthcare provider. In fact, such disclosures should be possible in Finland (through the centralised Kanta Services) in the future, under certain circumstances specified in the Finnish Act on the Electronic Processing of Client Data in Healthcare and Social Welfare.[105]

Health data in 'self-check' surveys

The EDPB's example 3 concerns information that an individual provides in a survey. The WP29 mentions online questionnaires in its guidance concerning health data in apps and devices, which is useful in interpreting the EDPB's case example 3.[106] Put into today's context, such a survey could, for example, be an online survey for assessing possible Covid-19 symptoms or the need for a Covid-19 test due to Covid-19 exposure. In light of the guidance from the EDPB and the WP29, here the context and purpose of use of the data are particularly relevant: the survey is provided and used to assess whether the person may have coronavirus and perhaps to provide advice based on the answers given. It is clear from the EDPB's example that the questions in the survey should be related to health. While the answers may include information about diseases and symptoms, even the input data that are not health data due to its content should be considered health data. Thus, an answer stating that the person has no symptoms and feels completely healthy is as much health data in this

[102] European Data Protection Board (n 11) 5. This list of examples is directly from this EDPB guidance.

[103] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 5. This summary is directly from this WP29 guidance. According to this WP29 guidance (on page 2), medical data refers to 'the category of data about the physical or mental health status of a data subject that are generated in a professional, medical context'. However, it should be noted that the GDPR does not define the concept of medical data. In principle, the concept needs to be analysed in light of the applicable national legislation, as the processing of medical data may be regulated on a national level. See art 9(4) of the GDPR, according to which the EU Member States may maintain or introduce further conditions with regard to the processing of health data.

[104] For further reflections about the comparison between the EDPB's and the WP29's guidance regarding data concerning health, see Schäfke-Zell (n 17) 4–5.

[105] See ss 13 and 20 of the Finnish Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021). The Act entered into force on 1 November 2021 and repealed the Act (159/2007) with the same name. See Ministry of Social Affairs and Health, Press Release <https://valtioneuvosto.fi/en/-/1271139/enablers-of-social-welfare-services-obliged-to-join-kanta-services-new-act-on-electronic-processing-of-client-data-in-healthcare-and-social-welfare-enters-into-force-on-1-november-2021> accessed 11 July 2022.

[106] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 2.

context as information about symptoms.[107] Any input data are health data because they are included in a health-related survey. The decisive factor here is the context and purpose of the data processing.

Finally, the most interesting and challenging cases correspond to the EDPB's examples 2 and 4. They refer to cases where information becomes health data due to how it is processed or due to the context in which it is processed. The use of the verb 'become' implies that in both examples the data are originally not considered health data. Instead, the datasets, which collectively form a data flow, transform into health data at some point of their lifecycle. This is because the data are either cross-referenced with other datasets or used in a certain context and for specific purposes.

When data become health-related due to cross-referencing

If the EDPB's example 2 is read together with the WP29's summary (in particular number 2 above) and other relevant WP29 documentation,[108] then data may become health data if they are combined, cross-referenced, or linked with other datasets, and this combination of datasets reveals something about the person's health. Typically, Qualified Self Devices combine datasets to provide useful insights, feedback, and recommendations to the user. Here, the input data become health data because they are combined with some other datasets (such as received or observed data), and the output data (inferred or predicted data) reveal something about the user's health.

The wording in example 3, however, does not clearly express whether the datasets must be combined or cross-referenced, or whether conclusions about health status must be drawn, to be considered health data. However, category 2 in the WP29's summary clearly indicates that it is enough that the data 'can be used' in itself or in combination with other datasets to draw conclusions, whereas the WP29's category 3 refers to cases where conclusions are drawn about a person's health status.[109] Thus, the WP29 is of the view that the mere possibility of combining datasets should fulfil the criteria of health data—it is, however, required that conclusions about the user's health data can be drawn based on the possible data combination. This also implies that the concept of health data does not require an intention to draw conclusions about health. It should, however, be noted that this topic—that is, whether there has to be an intention to reveal information about one's health and whether the data need to be reliable—is strongly debated.[110] The risk in WP29's approach is that, considering today's advanced technology and future developments, health-related conclusions can be drawn from any personal data.

According to the WP29's summary (category 3), it is further irrelevant whether the conclusions about a person's health status are accurate, legitimate, or adequate. The WP29 has also clarified that the term disease risk refers to data that concern an individual's potential future health status and cover any information 'where there is a scientifically proven or commonly perceived risk of disease in the future', such as obesity and high or low blood pressure.[111] This implies that the concept of health data has a broad scope and the link between any conclusions and actual disease risk does not need to be airtight. Again, this may result in all personal data being health data in practice.

Nevertheless, the WP29 has stated that 'data from which no conclusions can be reasonably drawn about the health status of a data subject' is in general not health data.[112] The use of the term 'reasonably' is reminiscent of GDPR's recital 26, according to which 'account should be taken of all the means reasonably likely to be used' to determine whether a natural person is identifiable. In light of the CJEU's arguments regarding the concept of personal data (under the Data Protection Directive) in *Breyer*, to fall outside of this criterion would basically require that identification is either prohibited by applicable legislation or 'practically impossible', as the identification would require 'a disproportionate effort in terms of time, cost and manpower'. In such a case, the risk of identification would appear to be 'insignificant'.[113] Interestingly, Advocate General Pikamäe noted, in his opinion (case *Vyriausioji tarnybinės etikos komisija)* regarding the definition of special categories of personal data, that it is relevant to consider the definition of 'identifiable natural person', who can be identified either directly or 'indirectly'.[114] Considering the WP29's reasoning and the CJEU's case law regarding the concepts of personal data and data concerning health, one could argue that the conclusions about health could be assessed similarly to the criterion of identifiability in the concept of health data. This would require consideration of all objective factors,

[107] Ibid.

[108] Ibid 4–5; Article 29 Working Party (n 78) 7.

[109] See Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 4–5.

[110] Wachter and Mittelstadt (n 16) 564–565.

[111] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 2.

[112] Ibid 3.

[113] *Breyer*, Case C-582/14, [2016] (ECLI:EU:C:2016:779) para 46. See also Bygrave and Tosoni (n 79) 111.

[114] Case *Vyriausioji tarnybinės etikos komisija*, Opinion of AG Pikamäe (n 53) para 87.

such as the available technical measures to construe a link between the dataset and the user's health. Yet again, such an approach would very likely lead to an interpretation according to which all personal data are health data.

A concrete example of wearable devices and the dilemma of health data is the recent decision by the Finnish supervisory authority, in which the Finnish supervisory authority imposed an administrative fine of EUR 122,000 on a company, a manufacturer of wearable heart rate monitoring technology, for processing health data without the appropriate consent required by the GDPR. The Finnish supervisory authority acted as the leading supervisory authority and the decision concerned several EU/EEA Member States.[115] As to the nature of the data, the Finnish supervisory authority noted in its decision that data on heart rate, as well as data on maximal oxygen uptake and body mass indices, are health data, and based on its reasoning in particular on the WP29's 'Annex – health data in apps and devices'.[116] Regarding heart rate, the Finnish supervisory authority pointed out that heart rate data combined with the other data processed by the company reveals information about the data subject's health. The company also processes data on, among other things, age, gender, weight, maximum heart rate, and resting heart rate. The WP29 has stated the following: '(. . .) 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 (. . .).'[117]

Certain contexts transform data into health data

Finally, the EDPB's example 4 is about data that become health data because they are used in a certain health-related context, such as information regarding a recent trip to or presence in a region affected by Covid-19 that is processed by a medical professional to make a diagnosis. The EDPB does not clarify which contexts or purposes, other than a healthcare context in conjunction with a medical purpose, may transform the data into health data. The EDPB's example 4 suggests that in principle, any data—regardless of their nature—may one day become health data if they are processed in a certain context.

The GDPR acknowledges that the context impacts the classification of data, as its recital 51 states that '[p]ersonal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms'. Even though the recitals are not binding, recital 51 indicates that the context of the processing should be considered in assessing the sensitivity of personal data.

A contextual approach is present in the ECtHR's reasoning regarding important elements of private life and processing of personal data that falls within the so-called 'personal sphere'. In *S and Marper v the United Kingdom*, delivered by the ECtHR's Grand Chamber, the ECtHR noted that '(. . .) in determining whether the personal information retained by the authorities involves any of the private-life aspects (. . .), the [ECtHR] will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (. . .)'.[118] Among the private-life aspects, the ECtHR mentioned information about the person's health and referred to, *inter alia*, its case *Z v Finland.*[119]

In *Z v Finland*, which concerned medical data, the ECtHR explained that respecting the confidentiality of health data is 'crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general'.[120] The ECtHR further noted the following: 'Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment

[115] The website of the Office of the Data Protection Ombudsman <https://tietosuoja.fi/-/terveystietoja-ilman-asianmukaista-suostumusta-kasitelleelle-yritykselle-seuraamusmaksu?languageId=en_US> accessed 20 February 2023. The decision of the Finnish supervisory authority is only available in Finnish: Tietosuojavaltuutetun ja seuraamuskollegion päätös, Dnro 1198/161/2022, 27 December 2022 <https://tietosuoja.fi/documents/6927448/146469002/Tietosuojavaltuutetun+ja+seuraamuskollegion+p%C3%A4%C3%A4t%C3%B6s_1198.161.2022.pdf/28156a55-c4f4-c47c-bd2b-a51e138ae4d7/Tietosuojavaltuutetun+ja+seuraamuskollegion+p%C3%A4%C3%A4t%C3%B6s_1198.161.2022.pdf?t=1673361700932> accessed 20 February 2023. See also the website of the European Data Protection Board <https://edpb.europa.eu/news/national-news/2023/finnish-sa-administrative-fine-company-processing-health-information_en> accessed 20 February 2023.

[116] The decision of the Finnish supervisory authority (n 115) paras 108–111 and 125–139; Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1).

[117] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 4; The decision of the Finnish supervisory authority (n 115) paras 110–111.

[118] *S and Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 67.

[119] Ibid para 66.

[120] *Z v Finland* (n 57) para 95.

and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community (. . .)'.[121]

Furthermore, as noted by Moerel and Prins, '[p]ractice shows that the same data may be sensitive in one context but not in another context (particularly when data are combined)'.[122] I agree that the use of personal data and the context of the processing should be considered when assessing the sensitive nature of the data. As the concept of health data is a dynamic concept and any data can transform into health data, the focus should be on data flows rather than on individual datasets.[123]

Surprisingly, the contextual approach was barely apparent, or at least little in evidence, in the CJEU's reasoning in *Vyriausioji tarnybinės etikos komisija*. The CJEU did not analyse the specific circumstances of the processing in this case. It is therefore unclear whether, or to what extent, the context of the processing had an impact on the CJEU's conclusions regarding the sensitive nature of the data.[124]

Four-step health data assessment

Based on the analysis in the previous sections of this article, this section proposes a four-step model, a health data assessment, which consists of the following elements: (i) content; (ii) context and purpose; (iii) usage; and (iv) effect. This model is a combination of the CJEU's reasoning in *Nowak* (content, purpose, effect) and in *Vyriausioji tarnybinės etikos komisija* ('intellectual operation involving comparison or deduction'), the WP29's guidance regarding personal data (content, purpose, result), and the EDPB's guidance concerning the concept of health data.[125] As the analysis of the concept of health data in 'Health data as a concept' section shows, the key is to define whether the personal data 'relates' to the health status of the natural person. Therefore, the reasoning in *Nowak* (and the WP29's three-step model) should, in my view, be applicable to the health data assessment.[126] Further, the CJEU's reasoning in *Vyriausioji tarnybinės etikos komisija* and the EDPB's examples of health data suggest that the context and the usage of the data should be considered as well.

This health data assessment focuses on data flows and considers not only input data but also output data. As in the WP29's model (content, purpose, and result) concerning personal data, it is enough that one of the elements indicates that the data are health data.[127] In this case, though, there is one exception, and that is step 4. To be considered health data, the data need to have some connection to the person's health status. Therefore, the effects of the data processing alone should not be sufficient to be considered health data. Further, in unclear cases, it is necessary to go through all four steps. This four-step model is demonstrated with the following examples of data: heart rate, body temperature, and number of steps taken.

Content

Considering the GDPR's wording, it is unclear whether a user's heart rate and body temperature (both observed data) fall within the GDPR's definition of health data. However, in light of the WP29's clarifications, information about heart rate alone, for example, should not be considered health data if the data fall within a normal range.[128] However, one could ask how it is possible to determine whether a certain value is within a normal range without any additional information. For the purposes of this example, let us assume that the data fall within a normal range. If the concept of health data is analysed along the lines of the Explanatory reports from 1981 to 2018 to Convention 108, then it also covers data that indicate that the person is healthy.[129] Similarly, the WP29 has acknowledged that the scope of health data is not limited to 'ill health'.[130] Could an 'intellectual exercise', as expressed by Advocate General Pikamäe (see 'Health data as a concept' section), result in the conclusion that the person is healthy and therefore their heart rate and body temperature data should be considered

[121] Ibid.

[122] Moerel and Prins (n 66) 57, 11.

[123] Ibid. The EDPB has noted that the context 'relates to the circumstances of the processing, which may influence the expectations of the data subject (. . .)'. See European Data Protection Board (n 18) 9. See also Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP 203, 2 April 2013) 24–25; Lee A Bygrave, *Data Privacy Law - An International Perspective* (OUP, Oxford, UK 2014) 156, 165; Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press, Stanford, United States 2010). According to Helen Nissenbaum, contexts include activities, norms, roles, and values. By values Nissenbaum refer to purposes and goals. Nissenbaum further notes that 'values are crucial, defining features of contexts'. According to Nissenbaum's theory of contextual privacy, the right to privacy is 'a right to appropriate flow of personal information'. Nissenbaum's approach is particularly useful in a data protection context, as it considers data flows and should also cover output data. Nissenbaum ibid 127, 132, 134. See also Pöysti (n 99) 195–97.

[124] See case *Vyriausioji tarnybinės etikos komisija* (n 48) paras 117–128.

[125] Article Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11); European Data Protection Board (n 11).

[126] See case *Nowak* (n 15) paras 34–62.

[127] Article Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11) 11.

[128] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 4.

[129] Council of Europe (n 40) ch II, Art 6 (para 45); Council of Europe (n 22) ch II, Art 6 (para 60).

[130] Article 29 Working Party, 'Annex - Health Data in Apps and Devices' (n 1) 2.

health data? In my view, this is unclear and further examination in step 2 of the model is therefore necessary.

Regarding the number of steps taken, the WP29 has stated the following: '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'.[131] The European Commission has taken a similar approach in its Draft Code of Conduct on privacy for mobile health applications, according to which such data (steps during a single walk) are 'merely lifestyle data'.[132] I argue that, by means of an intellectual exercise, it is impossible to draw any conclusions on the person's health solely on the basis of the number of steps taken during a single walk. Thus, it can be concluded that the number of steps taken during a walk should not, alone, be considered health data and further assessment of health-related elements is needed.

Context and purpose

In this example, the contractual relationship is between the service provider (the controller) and a consumer (the data subject), the processing concerns well-being data which are collected for the provision of the service, and the use of the service is voluntary.[133] Typically, the company that provides the service, including the device, provides the user with observations and recommendations that are based on the user's personal data (input data). This helps users to maintain or improve their lifestyle and well-being, inspiring them to live more healthily and to achieve their goals.[134]

The aim for which data are collected is the 'raison d'être' of the data processing.[135] In this context, the 'raison d'être' is to provide data to users about their well-being, so that they may monitor their lifestyle and well-being. Thus, the purpose is, at least indirectly, to contribute to the user's well-being. As we have seen in 'Health data as a concept' section, well-being and health are closely related.

Considering the broad scopes of both the concept of health and the concept of health data (as described in 'Health data as a concept' section), the purpose of the processing and the intended purpose of the device and the service provided by the company, I argue that any well-being data that are processed for the provision of the service are likely to be considered health data in this context. This applies to heart rate and body temperature as well as information about mood, steps, activities, and so on. If the device collects data about the user's alcohol consumption, exercise, and mood, then this is most likely for the purpose of providing the service. If this is not the case, then one could ask why such data need to be collected in the first place. GDPR's data minimisation principle requires that data collection must be limited to the data that are necessary for the purposes for which the data are processed.[136] To confirm the conclusion, namely that the data are likely to be considered health data, the following component (usage) is assessed as well.

Usage

In the context of Qualified Self Devices, many different datasets (such as heart rate, body temperature, steps taken, weight, and height) are typically combined with other datasets and measured over time. Considering the guidance from the WP29 and the EDPB as well as the CJEU's case law, the fact that datasets are combined or compared with each other, or that certain factors are measured over time, indicates that the data flow may transform into health data at some point.

A recent scientific study shows that a wearable smart ring (Oura Ring) could be used for early detection of Covid-19. The study notes that '[c]onsumer wearable devices that continuously measure physiological metrics hold promise as tools for early illness detection'.[137] This study is a brilliant example of how input data about well-being can be used to make conclusions about the user's health status. Considering the CJEU's reasoning, Advocate General Pikamäe's opinion as well as the EDPB's guidance, it is likely that well-being data are considered health data when they are combined or compared with other data. This interpretation is further supported by the example of the scientific study. Also, inferred data that are based on observed data, such as heart rate and body temperature, are likely to be health data if such datasets are combined or these parameters are measured over time.

[131] Ibid (n 1) 3.

[132] European Commission, 'Draft Code of Conduct on Privacy for Mobile Health Applications' (7 June 2016) 2 <https://digital-strategy.ec.europa.eu/en/library/code-conduct-privacy-mhealth-apps-has-been-finalised> accessed 14 July 2022.

[133] Regarding the context, see *S and Marper v the United Kingdom* (n 118) para 67; Article 29 Working Party (n 123) 24; European Data Protection Board (n 18) 9; Bygrave (n 123) 156.

[134] European Commission (n 33) 3 (footnote 2); Fitbit (n 35).

[135] Article 29 Working Party (n 123) 11.

[136] GDPR, Art 5(1)(c).

[137] AE Mason and others, 'Detection of COVID-19 Using Multimodal Data from a Wearable Device: Results from the First TemPredict Study' (2022) 12 Scientific Reports 3463.

To conclude, the assessments carried out in steps 1, 2, and 3 support the interpretation according to which lifestyle and well-being data, such as heart rate, body temperature, and number of steps taken, are most likely considered health data in this context. For the purposes of this article, the last step is briefly described as well.

Effect

The final step of the health data assessment is to examine the possible effects of the data processing. In line with the WP29's guidance concerning personal data, the question is whether the use of the data is 'likely to have any impact' on the data subject's rights and interests.[138] Thus, if the data subject were to be treated differently from other individuals due to the data processing, the effect (or result) element would be present.[139] For example, if a user of the Quantified Self Device is treated differently from other users, then this may indicate that their personal data are being used to draw conclusions on their lifestyle or well-being. In fact, this leads us back to step 3 (usage) of the health data assessment. The different steps of the assessment are closely linked to each other.

Concluding remarks

The previous sections show that the GDPR, with the CJEU's case law and the guidance from the EDPB and the WP29, provides valuable components to assess whether data are health data or not. However, they allow different interpretations and lack precision. Also, the relevant components of health data are embedded in several different sources, which makes it challenging to get a full picture of the concept. This article gathers those elements together in a structured way and makes a deep dive into the relevant legal sources. Further, the health data assessment introduced in section 'Four-step health data assessment' of this article seeks to provide a clear and logical way to assess whether lifestyle and well-being data are considered health data under the GDPR. To do so, it is important to understand the pillars of the concept ('personal data', 'concerning', 'health') and examine the concept's different dimensions.

This article shows that the lifestyle and well-being data processed by Quantified Self Devices for the purposes of providing the service (including the device) are, in principle, likely to fall within the scope of the GDPR's definition of data concerning health. The data flows include received and observed data as well as inferred and predicted data. Lifestyle and well-being data may allow either direct or indirect conclusions about the user's health. This is mainly due to the context and purpose of the processing, as well as the usage of the data. Some of the datasets are already health data due to their content. However, the content-centric approach to data categorisation is problematic in cases where the nature of the data is not particularly sensitive but the purpose of use, the context in which they are processed, or the way the data are used transforms the data into sensitive health data.

In light of the CJEU's case law, the concept of health data should be given a wide interpretation. However, in my view it should also be considered that the data categorisation may lose its fundamental point if the concept of health data is interpreted too broadly, covering in principle all personal data. As data are in constant movement, the health data assessment should focus on data flows. Datasets can no longer be assessed without considering the circumstances surrounding the data. Thus, the context and the purpose of the processing, the usage of the data flows, the content of the datasets, as well as possible effects form a complete picture of the health data flows.

Acknowledgements

The author would like to thank her supervisors Päivi Korpisaari, Professor in Communication Law (University of Helsinki), and Tuomas Pöysti, Doctor of Laws and Docent in Administrative Law (University of Helsinki), for their valuable comments during the writing process of this article.

Funding

The author would also like to thank the Eino Jutikkala Fund of the Finnish Academy of Science and Letters for the grant awarded to the author for her doctoral research.

Conflict of interest

The author is a data protection and privacy legal counsel in a corporate group which is a provider of healthcare and social care services. The group also provides digital healthcare software solutions through its subsidiary. Prior to her current role as an in-house lawyer, the author was employed by a Finnish law firm, and her tasks included advising corporate clients on matters relating to data protection, health technology and healthcare as well as other corporate law matters.

https://doi.org/10.1093/idpl/ipad007
Advance Access Publication 30 May 2023

[138] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 11) 11.

[139] Ibid.