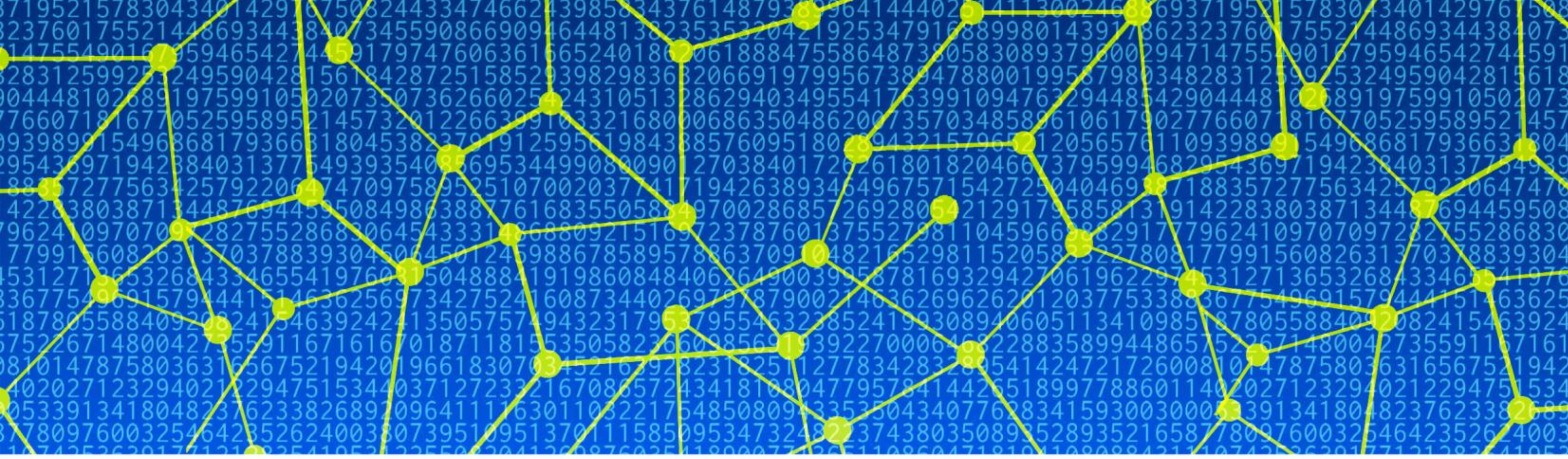

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 1/2015

Mobile Health

Reconciling technological innovation with data protection

21 May 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Mobile Health ("mHealth") is a rapidly growing sector stemming out of the convergence between healthcare and ICT. It includes *mobile applications* designed to deliver health-related services through smart devices often processing personal information about health. mHealth applications also process a large volume of *lifestyle* and *well-being* information.

The mHealth market is complicated because many public and private operators are active at the same time, for example app developers, app stores, devices manufacturers and advertisers, and the business models they adopt continuously shift and adapt to fast changing conditions. None the less, if they process personal information, they have to respect the data protection rules and be accountable for their data processing. Moreover, health information enjoys a very high level of protection under these rules.

The development of mHealth has great potential for improving healthcare and the lives of individuals. In addition, Big Data, together with the "Internet of Things" is expected to have a significant impact on mHealth because of the volume of information available and the quality of inferences that may be drawn from such information. It is expected to provide new insights for medical research and it might also reduce costs and simplify patient´s recourse to healthcare.

At the same time, it is necessary to protect individuals' dignity and fundamental rights, particularly those of privacy and data protection. The wide use of Big Data can reduce users´ control over their personal information. This is partly due to the huge unbalance between the limited information available to people and the extensive information available to entities which offer products involving the processing of this personal information.

We believe that the following measures relating to mHealth would bring about substantial benefits in the field of data protection:

- the EU legislator should, in future policy making measures in the field of mHealth, foster accountability and allocation of responsibility of those involved in the design, supply and functioning of apps (including designers and device manufacturers);
- app designers and publishers should design devices and apps to increase transparency and the level of information provided to individuals in relation to processing of their data and avoid collecting more data than is needed to perform the expected function. They should do so by embedding privacy and data protection settings in the design and by making them applicable by default, in case individuals are not invited to set their data protection options manually, for instance when installing apps on their smart devices;
- industry should use Big data in mHealth for purposes that are beneficial to the individuals and avoid using them for practices that could cause them harm, such as discriminatory profiling; and
- the legislator should enhance data security and encourage the application of privacy by design and by default through privacy engineering and the development of building blocks and tools.

Although mHealth is a new and developing sector, the EU data protection rules - as currently enacted and as will be further strengthened by the reform - provide safeguards to protect individuals´ data. At the same time, we will encourage the Internet Privacy Engineering Network (IPEN) to test new best practices and innovative solutions for mHealth. Also, considering the global dimension of data processing within mHealth, reinforced cooperation between data protection authorities around the world is crucial.

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 41(2) and 46(d) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION AND BACKGROUND

I.1 Background on mHealth - social benefits and Big Data

1. At the beginning of the years 2000 the media, IT and electronic communication industries began to converge, creating both a new business environment and new regulatory issues. Similarly, today, the healthcare industry has found new opportunities for development and growth in the convergence with new technologies (smart devices and related mobile apps). This combination aims ultimately at administering healthcare to users through smart devices, and is considered as an "*emerging and rapidly developing field which has the potential to play a part in the transformation of healthcare and increase its quality and efficiency*"[1].

2. The convergence between technology and healthcare is expected to allow (i) better healthcare at a lower cost, (ii) patient empowerment (*i.e.* improved control over own healthcare)[2], and (iii) easier and more immediate access to medical care and information online (*e.g.* by enabling doctors to remotely monitor patients and more often interact with them via e-mails).

3. The achievement of such objectives will be possible through the design and distribution of mobile devices (*e.g.* wearable computing devices) and apps running on users´ smart devices. They can capture increasing quantities of personal data (storage and computational power grow exponentially, as their price decreases) from a high number of "data sensors", which could be further processed in the providers´ datacentres with unprecedented computing capacity. The combination of ubiquitous use and connectivity, profit-making services often offered free to users (especially free mobile apps), together with Big Data and data mining plays a crucial role in mHealth, building a digital image of each of us (so-called *quantified self*)[3].

I.2 Aim of the Opinion

4. In view of the impact the development of mobile Health ("mHealth") may have on individuals' rights to privacy and personal data protection, we have decided on our own initiative to issue this Opinion.

5. It aims at drawing attention to the most relevant aspects of data protection for mHealth, which might currently be overlooked or underestimated, in order to enhance compliance

[1] European Commission Green Paper on mobile health, 10 April 2014, COM(2014) 219 final, complemented by a Staff Working Document (SWD(2014) 135 final).

[2] Nathan Cortez, *The Mobile Health Revolution?*, *University of California Davis Law Review*, Vol. 47, p.1173.

[3] Kelvin Kelly, founder of *Wired*, established the platform *quantifiedself.com* with journalist Gary Wolf, and introduced the concept to a broader audience.

with existing data protection rules and open the way to a consistent application of those rules. In doing so, it draws upon the opinion adopted by the Article 29 Working Party on mobile apps installed on smart devices[4].

6. It also considers the implications of this new, fast-changing scenario in view of the changes contemplated in the proposed General Data Protection Regulation ("GDPR").

7. This Opinion consists of two sections. Section II highlights the most relevant data protection implications of mHealth. Section III explores ways forward for the integration of data protection requirements in the design of mHealth apps. It does so by emphasising further legislative action which appears at the same time desirable and necessary to provide an effective response to the issues that mHealth is raising, or is likely to raise in the future, in terms of dignity, privacy, data protection and the right to personal identity.

II. DATA PROTECTION IMPLICATIONS OF mHEALTH

II.1 Requirements imposed by the EU rules

8. Privacy and protection of personal data are fundamental rights under Articles 7 and 8 of the EU Charter of Fundamental Rights[5]. In addition there are specific rules currently applicable to mHealth laid down in the Data Protection Directive[6] and the ePrivacy Directive[7]. These require that any processing of personal data must respect certain safeguards, for example the requirements that personal information may only be processed for specific purposes (purpose limitation) and should not be transferred to a destination outside the EU which does not offer an adequate level of protection (international transfers). In particular, information relating to health enjoys a higher level of protection and may not be processed unless certain conditions are satisfied, in particular the specific and informed consent of the user[8].

II.2 Definition of the types of data processed in the context of mHealth

9. The first question that needs to be answered is whether information processed in mHealth are personal data concerning identified or identifiable natural persons and therefore fall under the data protection legal framework. If so, it must then be determined whether, and which of those, must be considered as data relating to the health of an individual and, thus, fall under stricter data protection rules applicable to special categories of data. The

[4] Article 29 WP Opinion 2/2013 of 27.2.2013 on apps on smart devices (WP 202), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf .

[5] On the difference between the two distinct fundamental rights in Articles 7 and 8, see EDPS Guidelines on data protection in EU financial services regulation, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_EN.pdf.

[6] 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 L 281, 23.11.1995, p. 31–50.

[7] 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), OJ L 201, 31.7.2002, p. 37–47.

[8] Article 8 of the Directive prohibits the processing of special (*i.e.* "sensitive") categories of data, including health data, subject to a number of exceptions, to be interpreted narrowly.

question becomes particularly relevant in relation to the large volume of lifestyle and well-being information that is often shared on smart devices and social applications[9].

Data processed in context of mHealth are personal data

10. As to the first question above, it must be observed that **in principle, data processed in the context of mHealth are personal data** as they relate to identified or identifiable individuals (Article 2*a* of Directive 95/46/EC, hereinafter "the Directive").

11. Pseudonymisation and even anonymisation[10] do not fundamentally change the need to apply data protection safeguards to mHealth data. **Pseudonymous data remains personal data as it can be re-identified not only by the controller, but also by third parties through combination with external information from other sources[11].**

Are all data processed in mHealth to be treated as sensitive health data?

12. As to the second question, in many cases the data processed in the context of mHealth relate to, or reveal, the state of, physical (or mental) health of the individuals using the devices or apps[12], thus falling under the stricter data protection regime applicable to special categories of data (Article 8 of the Directive). However, there cannot be a simple definitive answer to this question: the assessment of which data processed in the mHealth field are sensitive health data can only be done on a case-by-case basis. **Lifestyle and well-being data will, in general, be considered health data, when they are processed in a medical context (*e.g.* the app is used upon advice of a patient's doctor) or where information regarding an individual's health may reasonably be inferred from the data (in itself, or combined with other information), especially when the purpose of the application is to monitor the health or well-being of the individual (whether in a medical context or otherwise).**

13. While the existing EU data protection framework includes provisions for the processing of sensitive data (including health data), it currently fails to provide a definition of health data (the situation is different at the level of single Member States)[13].

[9] According to the Commission Green Paper, mHealth covers "*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices*". This includes "*lifestyle and well-being apps that may connect to medical devices or sensors (e.g. bracelets or watches) as well as personal guidance systems, health information and medication reminders provided by SMS and telemedicine provided wirelessly*".

[10] Even when considered as anonymised, data may have intrinsic characteristics that lead to the identification of a specific individual (e.g. if a rare disease is at issue, in cases where a few patients exist worldwide, there is the risk that such patients are easily identified).

[11] See Article 29 Working Party Opinion 4/2007 of 20.06.2007 on the concept of personal data (WP 136), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, and Opinion 05/2014 of 10.04.2014 on anonymisation techniques (WP 216), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[12] Health data should also include administrative documents that include personal data relating to the health status of a person. Amongst those documents are medical certificates (*e.g.* documents certifying medical aptitude for work), forms concerning sick leave or the reimbursement of medical expenses. See EDPS Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, September 2009, p. 2.

[13] Additional details in the EU Commission First Report on the transposition of the data protection directive, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:en:NOT.

14. The General Data Protection Regulation (GDPR)[14], whose adoption is pending, provides for a definition of "*data concerning health"* as including *"any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual*"[15]. More interesting is the comprehensive, but non exhaustive, list included in recital (26) of the GDPR[16], which, nonetheless, does not specifically address the question whether and to what extent lifestyle and well-being information comes within the scope of health information.

15. The explanatory report of Convention 108 of the Council of Europe[17] provides that the term "personal data concerning health" includes "*information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased*". It is worth noting, in this respect, that the notion may also refer to healthy individuals (which would support the view that lifestyle and well-being information should be included as well, being that information capable of affecting the future health of a healthy individual).

16. **In the absence of a clear definition, after an assessment of the case-specific circumstances, the notion of what constitutes health data should be construed broadly**, so as to include any data relating to a person's physical and mental health information[18]. Due account must be taken of the fact that it is not only the intrinsic nature of the information that identifies it as health data. Also the circumstances surrounding the gathering and processing of such information play a role. As argued by a national data protection authority[19], there is not always a clear distinction between the notion of health data and well-being information. There is, rather, a *continuum*, from cases where well-being information has little or no relation whatsoever to individual's health to cases where -depending on the circumstances of data collection and processing, including its scale and the purposes of the processing- the information clearly constitutes health data and perhaps is even used in a medical context.

17. As a result, too narrow an interpretation of health data would deprive individuals of appropriate protection for their lifestyle and well-being information, which may reveal

[14] COM(2012) 11, final.

[15] GDPR, Article 4(1)(12).

[16] Recital (26) indicates that "*Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test*".

[17] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981, No 108.

[18] Both categories of data (lifestyle and well-being data) may involve the processing of personal data relating to health, thus triggering the higher standard of protection afforded by Article 8 of the Directive. See EDPS Opinion of 27.03.2013, on the Communication from the Commission on "*eHealth Action Plan 2012-2020-Innovative healthcare for the 21st century*", paras 10-11.

[19] Commission Nationale de l´Informatique et des Libertés (CNIL), *Le Corps, Nouvel Object Connecté`*, Cahiers IP no. 2.

very intimate information about them, and would risk forfeiting their trust and thus jeopardizing the economic and social gains mHealth would bring about[20].

18. In any event controllers of personal data are responsible and should be accountable in how they legally define the lifestyle information they process. In most cases, they are in possession of decisive elements to qualify such information as health data. Therefore, as the Article 29 Working Party has already noted, **in certain cases lifestyle data may "*provide information about the individual's health as the data is registered in time, thus making it possible to derive inferences from its variability over a given period. Data controllers should anticipate this possible shift in qualification and take adequate measures accordingly*"[21].** Such a rule efficiently places the burden of assessing the nature of the data processed (and, ultimately, compliance with the law) on the controller, the entity in possession of the best information[22].

Impact of the failure to identify and appropriately protect personal and sensitive data in mHealth

19. The Commission Green Paper on mHealth provides evidence of the magnitude of the risk of not protecting individuals. Recent estimates[23] quantify at 97,000 the mHealth apps currently available on multiple platforms, of which 70% target the consumer fitness and welfare and 30% target health professionals[24]. Is also expected that, by 2017, 3.4 billion people worldwide will own a smartphone and half of them will be using mHealth apps[25].

20. In contrast with the above figures, which depict booming trends -according to the Green Paper- only 23% of individuals have used any sort of mHealth solution. 67% does not intend to use their mobile phone in support of their health and 77% has never used their phone for health-related activities[26]. 45% of individuals are concerned about the unwanted use of their data when using their mobile phones for health-related activities[27]. Such concern is supported by the finding that nine of the top 20 health-related apps have been found to transmit data to companies tracking details about people´s mobile phone use[28].

21. The figures reported above identify lack of trust in mHealth as the main danger caused by lack of sufficient protection of mHealth users' data. **If the legislator, the regulators and controllers were to fail to properly identify personal and sensitive data (for example, taking the position that in no circumstance lifestyle information can be considered as**

[20] In the context of an initiative of the Global Privacy Enforcement Network (GPEN), data protection authorities have focused their attention on mHealth apps. See also Article 29 Working Party, in its letter to the Commission of 5 February 2015, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf .

[21] Article 29 Working Party Opinion on the Internet of Things, p. 17.

[22] The Article 29 WP provided some guidance on the definition of health data in its letter of 5 February 2015, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf .

[23] Research2Guidance (2013), "*The mobile health global market report 2013-2017: the commercialisation of mHealth apps*", Vol. 3.

[24] Deloitte study "*mHealth in a mWorld*", 2012.

[25] Research2Guidance, *cit.*.

[26] Bohem E., *Mobile Healthcare´s Slow Adoption Curve*, 2011, Forrester Research Inc.

[27] Blue Chip Patient Recruitment. *Leveraging Mobile Health Technology for Patient Recruitment*, October 2012.

[28] Financial Times, *Health apps run into privacy snags*, 1.9.2013.

sensitive health information), users would be deterred from using mHealth. Conversely, efficient data protection mechanisms will enhance user´s empowerment and engagement in mHealth[29].

II.3 A market with many players: allocating responsibility and ensuring users' empowerment

22. **The various actors of the mHealth industry -app developers, operating system (OS) manufacturers and device manufacturers, app stores and third parties (*e.g.* advertisers)- rely, although to a variable extent, on business models based on the monetization of personal data generated by (or concerning) users**.

23. As business models shift to new modalities of monetizing personal data (*e.g. platforms* and so-called *coopetition*[30]), it becomes increasingly difficult for users to control not only the *actual use* made of their data, but also the *re-use* of data by commercial partners of the controller and *potential use* that might take place once new possibilities of monetization become available due to the development of technology and business. For example, personal data originally disclosed to a patient association, in order to share information on a particular disease, might later be made available by such association to a pharmaceutical company which sells a medication for the disease and will use the information for commercial purposes. As highlighted in a previous Opinion of the EDPS[31], the dynamics of monetization are multiple and raise a number of serious data protection questions.

24. **In the first place, considering the multiplicity of parties involved in the mHealth industry and the different role played by each, it can be difficult to identify all controllers and processors and ensure an appropriate allocation of responsibilities.** The identification of the controller(s) of the processing carried out via mobile devices and apps is crucial to determine who is responsible for ensuring compliance with data protection law[32]. **Each entity must be transparent, visible, accountable, alone or jointly with others, for the handling of personal data it carries out.**

25. Second, it is difficult for individuals to be fully informed, and thus control, the actual use of their personal data, which, especially in businesses based on platforms (*e.g.* social networks), are transferred to, and processed by, various entities (device manufacturers, app publishers, platform operators and any other controller or processor). Because of the lack of transparency and scarce information on how their personal data are processed, individuals are in no position to express meaningful consent[33].

26. The problem is thus the *information asymmetry* existing between operators and users. On the one hand, market operators active in a number of sectors (healthcare, technology, advertising, insurance, etc.) will actively study all possibilities to exploit data in the context of new commercial initiatives and improve profits. On the other hand, users will

[29] EDPS Opinion on *eHealth Action Plan 2012-2020*, para 13.

[30] CNIL, *cit.*, p. 31. The key feature of this model is the platform operator´s ability to turn actual or potential competitors into commercial partners, shifting from business competition to so-called *coopetition*.

[31] EDPS Opinion of March 2014 on *Privacy and competitiveness in the age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy*.

[32] See Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, of 16.02.2010.

[33] Article 29 Working Party Opinion on apps on smart devices, p. 5.

have almost no visibility or understanding of the commercial dynamics that entail use of their personal information. **The increasing amount of data becoming available and processed as an effect of the tendency to rely on Big Data will only magnify the *information asymmetry* and increase the divide between controllers and users.**

II.4 The impact of Big Data on mHealth

27. Through the development of mHealth, Big Data is widely expected to have a significant impact on healthcare. **As it allows establishing connections -and thus extracting additional conclusions- from sets of previously unrelated data, Big Data will provide new insights for medical research, that were impossible to obtain before[34].** It will be possible, for example, to link diseases -such as obesity, cardiovascular diseases, depression- to human behaviour, lifestyle or other causes that are characteristic of a given geographic area or group of people.

28. Big Data may also facilitate decision making or collection of relevant information on the user side[35]. Nonetheless, it is in the commercial exploitation of the insights obtained through the combination of data that Big Data might have the greatest consequences for the individuals´ privacy (and raise major concerns).

29. Economic theory shows that a provider maximises profit when it is able to identify (and then, where appropriate, price-discriminate) between customers. In principle, if all patients remain unidentified, a pharmaceutical company will likely set a price for a drug which is the same for everyone. However, if the same company is able to identify who, among its customers, has more financial resources or has a greater need for the drug, it might be able to charge those customers a higher price (*e.g.* through a "premium" version of the drug that claims to be more effective). Big Data might facilitate such group discrimination. There is therefore a direct relationship between the availability of large sets of health data and the potential profitability of a number of industries active in the healthcare sector, as businesses will be able to better target their commercial propositions and thus draw a greater profit from the use of personal data. **In a self-reinforcing trend, greater chances of profit will turn into an even greater demand of data and greater need for effective safeguards against abuses.**

30. One of the most effective safeguards, in this respect, is making users aware of the purposes served by the processing of their personal data (*purpose limitation*). While it is mandatory to identify the purposes for which health data are processed, operators deploying mHealth solutions tend to resist tracking and limiting such purposes. This is because market dynamics evolve rapidly, steering businesses towards possibilities they had not considered before.

31. The wide availability of data and the possibility to process it in many different ways for commercial and scientific purposes will favour data duplication and maximisation, contrary to the principle of data minimisation set forth in Article 6 of the Directive. In this

[34] danah boyd and Crowford, Kate, *Six Provocations for Big Data*, (2011), p.3. "*Big Data is notable not because of its size, but because of its rationality to other data. Due to efforts to mine and aggregate data, Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself*".

[35] For example, a healthcare provider may have direct access to information about injuries an amateur athlete has suffered and provide her with a list of physicians who can assist the rehabilitation phase.

respect, purpose limitation and data minimisation go hand in hand. The more flexibility in the purposes of the processing, the harder to keep data to the minimum necessary (the proliferation in mobile apps will also contribute to a trend of data maximisation)[36].

32. Also, the interaction between the Internet of Things ("IoT")[37] and Big Data in mHealth can pose significant risks to data protection in view of the heavy penetration of smart devices and apps related to mHealth. Particularly relevant to mHealth are *wearable computing devices* which embed multiple interconnected sensors capable of recording body functions and lifestyle information. The quality of data produced by such devices and sensors may vary from merely raw data to more sophisticated data combinations and inferences concerning the data subject, revealing specific aspects of an individual's habits, behaviours and preferences[38], thus reinforcing the idea of the individual as a *quantified self* (*i.e.* digital projection of the individual).

33. The following example illustrates what can be understood by data minimisation: when designing a mobile app with the purpose of helping fight obesity, developers should ensure that it only collects the personal data necessary for that purpose. In that respect, although it might sometimes facilitate calorie tracking (*e.g.* by allowing users to scan the bar code of food they buy), further use by the operator of the information about users' preferences on product brands goes beyond the primary purpose of the app and thus would be excessive.

34. **Moreover the widespread collection of sensitive health data will open the door to profiling and possible adverse selection, for example for employment or insurance purposes.**

35. With respect to profiling, in the last few years, healthcare providers have used Big Data (including collection of genetic data) and algorithms to develop the so-called "predictive medicine", a discipline aiming at preventing future health risks based on present lifestyle (as reported by data). Insurance companies might also follow the same trend by sponsoring a number of programs to promote the use of monitoring devices and genetic screenings[39].

36. As to adverse selection, the concern is that, if all insurance companies and private healthcare providers adopt as a standard practice an in-depth monitoring of personal health data in order to adapt their commercial offering to each customer, they may automatically refuse coverage to those who object to such disclosure or sharing, regardless of their health conditions or risk factors. As a result, the practice of sharing

[36] Personal data collected through apps may be later distributed to undisclosed third parties for undefined purposes such as "market research". Recent studies show that massive quantities of personal data are collected through smartphones without any meaningful link to the apparent functionality of the app. See Wall Street Journal, *Your Apps Are Watching You*, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[37] Article 29 Working Party opinion about the Internet of Things ("Opinion 8/2014 on the Recent Developments on the Internet of Things"). "*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*".

[38] Article 29 Working Party opinion about the Internet of Things, p. 8.

[39] On profiling, see also Council of Europe, Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted on 23 November 2010, available at https://wcd.coe.int/ViewDoc.jsp?id=1710949.

data will automatically result in discrimination against those who prefer not to disclose or share their health data.

37. Possible distortions -especially data maximisation and profiling- caused by Big Data may be balanced, at least in part, by the correct application of the users´ right to object[40], as it will be further explained in section III.

II.5 Engineering mHealth apps: essential features

<u>Data security obligations</u>

38. As mentioned above, the lack of trust in mHealth will deter users from using innovative solutions and prevent society from reaping the benefits of mHealth. **It is therefore of the utmost importance for all operators to guarantee confidentiality, integrity and availability of the personal data processed according to data protection rules[41], international standards and best practices[42].** Among all possible options for information security, continuous risk management is the keystone to any security activity.

39. Although confidentiality of personal data is the most cited requirement, other security components - integrity and availability – are equally important when considering health information.

40. The scarcity of appropriate (*privacy-respectful*) tools and practices is an issue for all the technical parties involved in the development of mHealth devices and applications (*e.g.* app developers and device manufacturers). In a fast-evolving technological environment, developers have to deliver quickly their products so as not to be overtaken by competitors. Therefore, they may often re-use existing components, in spite of possible inherent privacy flaws. This may imply, unfortunately, few building blocks for privacy-friendly applications and services, often resulting into poor security. **In such a context, the application of *privacy-by-default* and *privacy-by-design* principles, combined with a systematic effort towards privacy engineering, is necessary to address the problem. The Internet Privacy Engineering Network (IPEN[43]) provides a framework in which these issues may be addressed in cooperation between engineers and legal and regulatory experts.**

[40] Article 14 of the Directive provides for such right, which is particularly important in the Internet era and in the mHealth domain. The Directive also mandates that data needs to be kept up to date (Article 6) and allows the data subject to object or block the processing of data which he finds inaccurate (Article 12). Healthcare conditions, in fact, change over time and individuals should not be associated to obsolete information.

[41] Like Article 17 of the Directive which mandates the application of information risk management to data processing.

[42] Article 29 Working Party, *cit.*, p. 14. As to the measures to take, app developers may refer to public security guidelines, such as the "Smartphone Secure Development Guidelines" published by ENISA and available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport.

[43] The Internet Privacy Engineering Network (IPEN) brings together developers and data protection experts from regulators, business, civil society and academia to work together on privacy respecting solutions for practical problems (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN). In this respect, we will encourage IPEN to make a test on mHealth and verify which best practices may be launched/evaluated/recommended by its community of engineers and experts.

Transfer of data abroad

41. **Because devices and apps are distributed at global level by healthcare and IT companies located outside of the European Union, data processing may often take place outside the Union´s borders.** In particular, the most relevant (and typical) scenario, for mHealth, would entail the processing of data in a global cloud environment, with data being transferred to third countries without any knowledge or control by the user, often under the responsibility of a controller located outside the EU or outside countries covered by a Commission adequacy decision.

42. A German insurance company collecting data on its customers´ risk in the EU may for instance share them later with another insurance company in Canada, in conformity with Article 25 of the Directive as Canada has been recognised as presenting an adequate level of protection under a Commission Decision[44] [45]. In other cases, however, data transfers may only take place subject to the criteria and safeguards provided by Articles 25 and 26 of the Directive[46].

III. WAYS FORWARD FOR THE INTEGRATION OF DATA PROTECTION REQUIREMENTS IN THE DESIGN OF mHEALTH APPS

III.1 Legislative framework

43. As developed above, in the context of mHealth many types of data available on smart mobile devices are personal data, and must thus be processed in accordance with the requirements of the data protection rules.

44. In addition, health data reveal intimate aspects of the individual and may also represent a significant intrusion into his or her privacy. In this respect, the right to privacy will have to be ensured, by replacing excessively intrusive measures with alternative, less intrusive options serving the same purpose.

Application of current rules applicable in the mHealth context

45. Mobile apps controllers as well as apps designers must take the data protection rules and, particularly, the sensitive nature of health data into account when designing their apps for mHealth.

46. **It is crucial, in particular, that controllers and processors make an effort to improve transparency on the way they process, share and re-use personal data as well as on**

[44] Commission Decision no. 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539).

[45] In such cases, the term "transfer" would therefore cover both "deliberate transfers" and "permitted access" to data by recipient(s). Illegal access and hacking would be excluded.

[46] See WP Opinion 3/2009 (WP 161) on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (controller to processor) and FAQs of 12.07.2010 addressing some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (WP 176), as well as WP opinions on BCRs and the Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

the purposes they aim at. The fact that a wide array of commercial purposes may lay behind the processing of personal health data does not exempt the controller from its responsibility to properly inform users, on the contrary: sufficient information should be communicated, so that they can provide a specific consent to the processing of their health data. Users´ freedom to choose and decide on the processing of their health data should not be limited as a consequence of the app design.

47. **In this respect, granting data subjects the choice to limit the processing of mHealth data locally -on their smart devices, rather than on a remote server- is one of the important safeguards mHealth apps and devices should implement. Also, giving individuals the option to freely allow the sharing/transfer of the personal data to a third party or not by the controller is an important feature all mHealth applications and devices should incorporate. All these options should be smart and easy to implement even by non-expert users, based on a clear and easy readable notice.**

48. **Designers and manufacturers should apply the same level of creativity and dynamicity they usually display in introducing attractive devices and apps to also provide individuals with effective and user-friendly privacy notices and setting options. As a result, individuals should be able to set options relevant to their privacy and data protection with the awareness that this is an important element of the devices and apps' use, in their own personal interest, and not a boring formality or a useless burden.**

49. In order to facilitate users´ control over their own data -as it happens sometimes with software running on personal computers-, when activating a mHealth device or application, the users should be able to easily decide if they want to set manually their data protection settings or rather accept/change the default settings, which should be set on a higher privacy and data protection standard (application of *privacy by default*). App developers should also model the data protection options included in the app on widely accepted data protection guidelines (*e.g.* those adopted by ENISA[47]).

50. It must be noted that, in some cases, the processing of personal data through mobile apps is also carried out by private users, which may become jointly responsible as controllers of the data they process. Such processing would not fall within the so-called *household exception*[48] in cases where the user of the app aims for instance at sharing widely personal data on the Internet (via a social network or a mailing list). The household exception should also be narrowly applied[49] in the sense that, regardless of whether the user meets its criteria, those organisations involved in the design, supply and functioning of the app (app designers, app store, and third parties) remain responsible for the processing they carry out in pursuit of their own purposes.

[47] Footnote 42, above.

[48] Article 3(2) of the Directive.

[49] Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, judgment of the CJEU of 11.12.2014, paras 29 ss.

51. As mHealth involves data processing through smart devices, it is worth noting that a valid informed consent of the data subject is a condition for the storing or access to information stored on the terminal equipment of a subscriber or user[50].

The GDPR: the "modernization" of the data protection framework

52. The GDPR, currently still a proposal though in an advanced stage of discussion, will introduce substantial changes concerning data protection online and impacting also on healthcare.

53. **In general, the GDPR aims to strengthen the rights of the data subjects, particularly in situations where interference with their right to privacy might be magnified by online interaction[51]. The GDPR also introduces new guiding principles and rules applicable in the context of mHealth[52].** For example, privacy by design and by default become legal obligations (and no longer mere "best practices") under the GDPR[53], and thus will have to be fully taken into consideration when designing new mHealth apps or devices.

54. As to the interaction between EU law and national law the GDPR seems to leave a substantial margin of manoeuvring to the national legislator[54]. In this respect, as long as the healthcare domain is concerned by the exercise of such discretion, we believe that **the adoption of national legislation should not prejudice the consistent application of EU data protection law by creating discrepancies instead of solving them.**

III.2 Additional measures aiming at reinforcing data protection safeguards in mHealth

Fostering accountability

55. A systematic approach to the challenges of mHealth demands that the responsible controller(s) is correctly identified and that responsibility is organised efficiently, in case various players on the market are involved in data processing[55] [56].

56. In this respect, we have explained in the paragraphs above how market dynamics are continuously developing into new business models, involving from time to time new entities and operators. In order to avoid that the fast growth of an articulated market environment evolves into a chaos, responsibility for any data processing should be allocated in a coherent and systematic fashion. Whoever holds an interest, or pursues a

[50] Article 5(3) of the e-Privacy Directive (No. 2002/58/EC), applicable to any entity that places on or reads information from smart devices, regardless of its nature (public or private, individual or corporation, controller or processor or third party) of such entity. See, also, Article 29 Working Party, *cit.*, p. 7.

[51] Examples include Article 11, Article 12 and Article 14.

[52] in particular: Article 4(12), which provides a definition of "data concerning health"; Article 20 on profiling (including health profiling and "predictive" profiling); Article 33 on the impact assessment of data processing (including "specific-risk" processing, such as that involving health data) and Article 81 on the safeguards for health data processing.

[53] Article 23 "Data protection by design and by default".

[54] EDPS Opinion on the data protection reform package, paras 50 ss.

[55] See WP Opinion 1/2010 of 16.02.2010 on the concepts of "controller" and "processor" (WP 169) available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[56] EDPS Opinion on the e-Health Action Plan 2012-2020, para 19. In this respect, we note that the GDPR provides for more specific rules on accountability, so as to allocate responsibility efficiently and make the right entity/ies accountable.

goal, related to personal data and therefore engages into data processing shall be accountable to users whose data are processed.

Ensuring the correct application of data protection rules

57. Although mHealth is largely a new phenomenon, both the Directive and the ePrivacy Directive set forth provisions able to protect the users´ rights. It must therefore be ensured -by policy makers, controllers and data protection authorities- that the data protection rules are correctly implemented in a proactive and responsible manner.

58. As indicated by the Article 29 Working Party, purpose limitation and data minimisation go hand in hand[57]. They both contribute to prevent unlawful re-use of personal information. As the current economic landscape evolves towards data re-use and intensive exploitation of data for multiple (at times, even unforeseen) purposes, it is crucial that the purpose of the processing is clearly identifiable by users and that protective measures are appropriately implemented by controllers, and that data disclosure and processing are kept to the minimum necessary.

59. It is clear, in this respect, that EU and national competent data protection authorities have a crucial role in monitoring the application of such rules and intervening when necessary. Furthermore, because of the global dimension of the processing, reinforced cooperation among data protection authorities worldwide, in the context of a coherent strategy, is crucial.

Promoting coherent application of data protection rules in the field of mHealth

60. Due account should also be given by the EU legislator and by mHealth stakeholders to guidelines providing standards for the processing of health data, such as the Article 29 Working Party opinion on the Electronic Health Records (EHR)[58], and the recommendation of the Council of Europe on the protection of medical data[59]. A code of conduct elaborated by mHealth stakeholders with the contribution of DPAs might also help fostering a coherent application of existing data protection rules in relation to mHealth.

Empowering individuals

61. One of the goals of developing mHealth is to enhance patients' *empowerment*, which consists of greater individual control over their healthcare.

62. We consider that a greater level of empowerment should be achieved also in data protection, by enhancing users' control over their personal data. App developers and stores should increase transparency to the benefit of individuals. Users should be better informed on processing of their data and allowed, timely and effectively, to give and/or revoke consent or opt out from processing where relevant. One very powerful mean to increase users' control is to grant them the possibility to process their own personal data strictly locally without any transfer to any provider.

[57] Article 29 Working Party Opinion on apps on smart devices, p. 17.
[58] Article 29 Working Party opinion of 15.02.2007, no. 00323/07/EN.
[59] Recommendation no. R (97) 5 of 13.02.1997.

63. In this respect, in a landscape of growing complexity, we also support data portability (and interoperability of formats and technologies) as a solution towards simplification, transparency and control by users and against data duplication.

Securing personal data and improving engineering requirements

64. The legislator should require that all actors guarantee confidentiality, integrity and availability of the personal data processed according to data protection rules, international standards and best practices. Among all possible options for information security, continuous risk management shall be the keystone to any security activity.

65. *Privacy-by-default* and *privacy-by-design*, combined with a systematic effort towards privacy engineering, need to be applied throughout the mHealth ecosystem. The legislator should encourage the adoption of tools for innovative privacy-friendly applications and services (libraries, design patterns, snippets, algorithms, methods and practices).

Safeguards for the use of Big Data in mHealth

66. Although Big Data has potential for bringing improvements to both the public and the private healthcare sector, it may also constrain data protection rights, especially through extensive data mining and profiling. It is therefore necessary that the legislator adopts rules that make data mining in the context of mHealth acceptable only in specific circumstances and provided that full account is taken of data protection rules.

67. Given that effective anonymisation of the data is very difficult to achieve, and that pseudonymous data remains personal data, any processing of large amounts of data for purposes of analysis must be subject to strict data protection safeguards. Furthermore, the persons who are authorised to access these data and the modalities for such access should be clearly identified.

68. The combination of data for purpose of building up profiles, while in some cases and when applied correctly (*e.g.* personalised medicine) may be highly beneficial for the individual, may also raise serious data protection concerns, in particular if it leads to other types of decisions being taken that may affect individuals (*e.g.* insurance companies may decide not to insure someone if they have access to the health profile of an individual they believe associated to a high probability of cancer)[60]. Hence, profiling, especially if it is not carried out merely for research purposes, with strict functional separation, but also aims at singling out and treating differently the individuals concerned, should only be done in very specific circumstances under an *ad hoc* legal basis and/or with the explicit consent from the data subject, and provided that strict data protection requirements are met (*e.g.* as set forth in Article 15 of the Directive and in Article 20 of the proposed GDPR). In addition, the data subject´s right to further object to data processing will stand as an additional safeguard.

[60] See Art 29 Working Party, Opinion on purpose limitation of 2.04.2013, available at http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf, "*In particular, an algorithm might spot a correlation, and then draw a statistical inference that is, when applied to inform marketing or other decisions, unfair and discriminatory This may perpetuate existing prejudices and stereotypes, and aggravate the problems of social exclusion and stratification*".

IV. CONCLUSION

69. mHealth offers a wealth of new opportunities, in terms of better and more responsive healthcare for individuals, better disease prevention and lower healthcare costs for welfare systems and greater opportunities for businesses. However, in order to achieve a situation where all the three categories above may fully benefit from these developments, everyone needs to accept the responsibilities that come with opportunities.

70. In particular, we draw the attention on the responsibility to individuals and to the need to preserve their dignity and their rights to privacy and self-determination. In a context of rapid economic change and dynamic interaction among various private and public operators, these fundamental principles should not be overlooked and private profit should not translate into a cost for society.

71. In this respect, data protection principles and rules provide guidance in a sector which is still largely unregulated. If duly complied with, they will increase legal certainty and trust in mHealth, thus contributing to its full development.

Done in Brussels, 21 May 2015

(signed)

Giovanni BUTTARELLI
European Data Protection Supervisor