

EUROPEAN DATA PROTECTION SUPERVISOR

Executive Summary of the Opinion of the European Data Protection Supervisor on 'Mobile Health: Reconciling technological innovation with data protection'

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2015/C 232/06)

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 patients' 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.

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 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.

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.

⁽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.

⁽⁴⁾ Article 29 WP Opinion 2/2013 of 27 February 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

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.

Giovanni BUTTARELLI
European Data Protection Supervisor
