Wojciech Wiewiórowski, Assistant EDPS, on mHealth at General Assembly of Association Internationale de la Mutualité, Liège, Belgium

Speaking notes

23 June 2015

We cannot allow new technologies to drive the values this culture is built on … even if the technologies give us wonderful tools to be healthier, smarter and they improve our well-being

Ladies and gentlemen ... Dear Data Subjects ,

First of all, let me thank you for your invitation. I am very glad to be here and to have the opportunity to share with you a few considerations on the way healthcare is evolving these days and on the implications that such change has on data protection.

EDPS

I particularly appreciate this opportunity, as I am aware that your mission is to defend the access to healthcare for all through solidarity-based and non-for profit health insurance. In this respect - although the EDPS is not a healthcare organisation - I believe we share the same concerns. We both would like to improve access of individuals to healthcare, whenever they need it, and we both would like the individual to be at the centre of all discussions and all concerns.

Access to healthcare and the relevance of human dignity are also subject of the mobile health Opinion that I would like to share with you today. In this Opinion, we address the delicate topic of defining and processing sensitive health information which, if misused, could seriously harm the individual. We also explore the way technology improves

access to healthcare services and, sometimes, makes them unnecessary, by educating individuals about prevention and guiding them towards a healthier way of living.

As we can easily understand by looking into the palm of our hand, electronic devices are becoming smarter and smarter and, in spite of the small size, more powerful. Their data storage and computing capabilities improve by the day as their price decreases. If well managed, new, inexpensive technology may deliver substantive social benefits in the healthcare sector, in terms of better disease prevention, better access to healthcare, less and better targeted medical intervention, lower medical expenditure and greater patients´ control over their health conditions.

Big data big responsibility

These benefits, however, will not come without effort. The combination (or convergence) between healthcare and smart technology opens up a number of questions and challenges we need to address, so that all categories (patients and other stakeholders) may benefit from mobile health and that the gain of one does not come at the expenses of the others.

Mobile Health (or mHealth), as we define it, relies on the delivery of a number of innovative healthcare and wellness services to final users through a growing number of smart applications running on our devices. These services depend on the collection and processing of users´ personal data. It is obvious that data collection and processing shall not only depend on market trends, but need rules and safeguards. Will rules and safeguards limit the growth of new healthcare solutions? We believe they won´t. Rather to the opposite, they will foster users´ confidence and engagement and provide a firm ground for mobile health to grow and expand.

Mobile health connects, directly or indirectly, users to a number of economic players, such as device manufacturers, app designers, healthcare service providers and advertisers, each processing personal data for its own purposes. We believe that users need to remain the centre of our concerns and in control of their data.

In fact, the social and economic costs of not ensuring proper data protection safeguards to mobile health users are relevant and are well described by the European Commission in its Green Paper on mobile health: by 2017 about 3.4 million people are expected to own a smart device, but only 23% have used mobile health solutions so far. 77% has never used mobile health application and 67% wants "nothing at all" on their phone for their health. These figures deliver the clear message that the benefits of mobile health will remain on paper, without users´ confidence and users´ confidence depends on effective data protection.

What is the opinion of DPA

For such reasons, in May we have adopted an Opinion on mobile health that takes a structured approach to mobile health and addresses what we consider the most immediate challenges and questions raised by this phenomenon. I encourage you to find the time to look at it on our website. Also, in the last months, we have been working on comments to the proposed General Data Protection Regulation in order to include in the legislative text clear guidance on the processing of health data and on Big Data in general.

Strange as it may sound, the main challenge we face is to give a proper definition of health data, in order to ensure that individual information is adequately protected. There are, at national level, several definitions of health data, but they have all been adopted for the purpose of sector-specific regulation. We lack, at EU level, a clear and comprehensive definition that would adapt to data protection purposes.

What is the future

The most pressing question, in this respect, is whether we shall include lifestyle and well-being information in the notion. This kind of information (e.g. sleep hours, running performances, eating habits, food preferences) is largely processed by smart mHealth applications and we believe should be certainly protected as health data when collected or processed in a health context or for health purposes.

Another challenge concerns basic accountability for data processing. As I mentioned, multiple entities - public and private, for profit or no-profit - may be involved in the processing of health data concerning users. Our position is that any entity that processes personal data for own purposes shall be accountable for that processing. That requires that data processing, in the context of mobile health, is transparent enough to allow users to retain control over their data, identify the entity processing their data, be aware of the way their data are processed and object to that processing if they choose to do so.

We have talked about basic principles, such as accountability and transparency, but there are other urgent concerns in relation to personal data, in particular data security. Data can be stolen, leaked or used improperly. We have to ensure that the development of adequate security solutions for our data go hand in hand with the development of innovative services. In this respect, we use the expression privacy-by-design to indicate an approach that, instead of mending privacy gaps ex post, seeks to integrate privacy and data security in the technology during the design phase. We also advocate privacy-by-default, which commands the application of acceptable privacy standards by default in case users are not able to select themselves the most appropriate safeguards.

Lens

I come now to discuss one of the most controversial aspects of mobile health, which is Big Data. As I mentioned before, personal data are more and more available and improving computing capabilities allow a fast processing of such large body of information. Big Data includes all technology solutions that allow exploring relations between sets of data that before were (or appeared) unrelated. Big Data opens new possibilities in science and medical research, as it allows the formulation of new conclusions from information that could not be processed before. Therefore, we expect significant progress in many fields thanks to the use of Big Data.

Wearables

However, we need to bear in mind that a large potential often brings with it similarly large responsibilities and, I think, this is the case of Big Data. In order to deploy its full effectiveness, Big Data needs large amounts of personal data and is thus likely to affect the most intimate sphere of individuals. For such a reason, the use of Big Data should be assisted by adequate safeguards and be in compliance with data protection rules.

Big Data, of course, opens also unprecedented profit opportunities for businesses relying on personal data in order to provide customised services to their customers. There is, in fact, a tight relationship between data availability and business profitability. The more data you have, the more sophisticate, targeted and customised your services can be. Similarly, the more you will succeed on the market, the more you will scan the Internet for additional data that will help you designing new services.

An anecdote will provide an excellent example of what I am saying: I once met an entrepreneur active in the business of smart white goods and he explained to me that personal data were the "food" of the smart devices he put on the market. However, as technology moves forward at a fast pace, he was forced, day after day, to source more detailed and comprehensive data to feed to his machines. He added that, in order to stay ahead of his competitors, he had to mine, from the Internet and from elsewhere, as many data as possible, sometimes even before knowing exactly what to do with them.

Nappies

Now, we certainly do not consider business as being evil nor we believe that Big Data should foster progress in any field but business. What we are concerned about - and I imagine you share my concern - is that the individual, with his personal data, becomes a commodity, a factor to be added in the profit equation, just like bank loans and interest rates. We have to remember, in this respect, that the right to privacy and data protection are fundamental rights of the individual which allow any of us - the hostess on the plane, the policeman on the street and the CEO of the fanciest technology start-up - to build our personality and to affirm ourselves as individuals part of a civil society and not as mere customers or users.

The need to strike a balance between data protection and other concurring interests poses important ethical questions. In this respect, I would like to borrow the word "empowerment" from the Commission´s Green Paper on mobile health. In that document, empowerment is described as one of the benefits of mobile health and refers to the fact that, thank to smart solutions, users and patients will be more active and more in control of their health, whether they are sick or not. We think that individuals should be empowered not only with respect to their health, but also in relation to their personal data.

Being empowered in relation to own personal data means acting in a transparent environment, where data processors provide correct information to users, so that users are aware of what is done with their data. It also means that users retain control over their data during the entire period their data is processed and are constantly informed of the purposes of such processing. It means they can object, if they wish so.

Privacy by design

The need to balance ethical and practical considerations leads me to mention a few key principles that are already embedded in the current data protection legislation and serve us as the basic tools to handle the challenges of mobile health. I just referred to the principle of correct and transparent information to users; I would also like to refer to the principle of purpose limitation, which does not prevent the processing of data, as long as the purpose of such processing is explicit and legitimate; the principle of data minimization that avoids massive collection of data in circumstances where this is not needed, and the principles of data security and privacy-by-design and privacy-by-default, whose relevance we have seen above. We think that these principles are at the core of the data protection culture and should not be forgotten as we enter a new economic scenario such as mobile health.

Big data big responsibility

In this respect, I would like to acknowledge the initiative of the European Commission that has launched a working group - gathering members of the healthcare and technology industries, data protection experts and regulators - in charge of drafting a code of conduct for app designers and providers of mobile health services. We think that providing clear guidance and spreading the culture of data protection will help mobile health to develop at its best.

To conclude, I am confident that you see now how effective data protection safeguards will allow mobile health to produce social benefits in healthcare. Technology has a large potential for improving users´ health (by spreading the culture of prevention) and access to healthcare, but needs to be associated to data protection safeguards in order

to deploy such potential in the right direction. It is clear that mobile health reveals very exciting perspectives ahead of us, for patients, for business and for governments. The economic landscape changes to the rhythm of the innovative technology that every day is brought to market, but we should not lose sight of how important individuals are and how important personal data and data protection are for the individuals.

Thank you for your attention