PRESS RELEASE

EDPS/2015/03

Brussels, Thursday 21 May 2015

Healthcare on the move

Mobile technology is revolutionising the healthcare market, offering opportunities to benefit the global population with a variety of healthcare needs, said the European Data Protection Supervisor (EDPS) today following the publication of his **Opinion** on **Mobile Health** (mHealth). However, as a society we should take care to identify and support solutions which **first and foremost serve individuals and respect their choices**. Such solutions should not only be technically feasible but also be **ethically tenable and foster trust**.

Giovanni Buttarelli, EDPS, said: *"We live in a world where our digital lives can be acutely analysed. Today, the **division** between information about our health and information about the rest of our digital lives is **disappearing**: technology solutions allow devices and apps to connect the dots between different data about us such as location, nutrition and medical.* We can put a lot of **trust** in technology companies to do the right thing with our personal information and to make our lives easier. *But we need to have a **critical debate** about the uses of our personal information that are and are not acceptable to us and encourage developers to prioritise consumer **trust** over short term gains."*

Better quality, low cost health care is associated with advances in technology and offers significant benefits for patients, health authorities and businesses. Mobile health technology can be broken down into two categories: wellness (for consumers and patients) and medical (for physicians). **Wellness and prevention are key in healthcare** and the EDPS Opinion on mHealth focuses on the technology for wellness.

Under current EU data protection rules, information about health enjoys a very high level of protection. But in the wellness market, it is **not entirely clear what would constitute health information** in practice. This is one of the areas that must be addressed.

Big Data is impacting mHealth in a big way. The potential to collect a huge amount of personal information (physiological, preferences, emotions and so on) and the potential to **buy**, **sell** and **analyse** it without the full knowledge and consent of the people concerned has to be addressed by industry and governments - and by us, as consumers of these technologies.

The ways and the purposes for which personal data is processed, shared and re-used must be made **transparent**, for instance through **easy-to-read privacy policies** which are **highlighted** rather than hidden away and a list from which you can **actively choose** to opt-in or out.

Failure to deploy **data protection safeguards** will result in a critical loss of individual **trust**, leading to fewer opportunities for public authorities and businesses, hampering the development of the health market. To foster confidence, future policies need to encourage more **accountability** of service providers and their associates; place respect for the choices of individuals at their core; end the **indiscriminate collection** of personal information and any possible **discriminatory profiling**; encourage **privacy by design** and privacy settings **by default**; and enhance the **security** of the technologies used.

The challenges of **privacy engineering** in mHealth technologies may be addressed within the Internet Privacy Engineering Network (IPEN) which provides a framework for cooperation between engineers, legal and regulatory experts; the EDPS will **encourage IPEN** to do so. **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.

Technology is designed to work for us, not the other way around. European society, our values and laws have been developed to protect and empower individuals, whether as citizens, users or entrepreneurs. We are not only consumers of goods and services. The **dignity** of future generations needs protecting. We need to **debate** and find **solutions** on how to stay **connected** on the move that also respect our **privacy** and personal identity.

More people are taking a **proactive** role in checking or monitoring their health than ever before. The enhanced power of ubiquitous new computing devices is helping to drive this growth. But individuals should not only be **empowered** to be proactive over health, they should be empowered over their personal lives as a whole. **Transparency**, **awareness** and effective **control over personal information** all contribute to such empowerment.

Background information

Privacy and data protection are fundamental rights in the EU. Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

More specifically, the rules for data protection in the EU institutions - as well as the duties of the European Data Protection Supervisor (EDPS) - are set out in **Regulation (EC) No 45/2001**. The EDPS is a relatively new but increasingly influential independent supervisory authority with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.

Giovanni Buttarelli (EDPS) and **Wojciech Wiewiórowski** (Assistant EDPS) are members of the institution, appointed by a joint decision of the European Parliament and the Council. Assigned for a five year term, they took office on 4 December 2014.

EDPS Strategy 2015-2019: Unveiled on 2 March 2015, the 2015-2019 plan summarises the major data protection and privacy challenges over the coming years; three strategic objectives and 10 accompanying actions for meeting those challenges; how to deliver the strategy through effective resource management, clear communication and evaluation of our performance. Our mHealth Opinion aims to provoke thought and launch a debate in the context of at least three of the actions laid out in our strategy: increasing transparency, user control and accountability in big data processing; the ethical dimension of data protection; and facilitating responsible and informed policymaking.

Personal information or data: Any information relating to an identified or identifiable natural (living) person. Examples include names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other details such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered as personal data.

Privacy: the right of an individual to be left alone and in control of information about his or herself. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter also contains an explicit right to the protection of personal data (Article 8).

Processing of personal data: According to Article 2(b) of Regulation (EC) No 45/2001, processing of personal data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." See the glossary on the EDPS website.

Big data: Gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms. See also Article 29 Working Party Opinion 03/2013 on purpose limitation p.35.

IPEN: The Internet Privacy Engineering Network brings together developers and data protection experts from regulators, business, civil society and academia to work together on privacy respecting solutions for practical problems.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy;
- cooperating with similar authorities to ensure consistent data protection.
