



Consultation on the legal framework for the fundamental right to protection of personal data

The following consensus document resulted from an internal discussion among partners of the two FP7 funded projects HIDE¹ (Homeland Security, Biometric Identification and Personal Detection Ethics, Grant Agreement nr 217762) and RISE² (Rising Pan European and International Awareness of biometrics and Security Ethics, Grant Agreement nr 230389). The text below has been agreed among all partners and reflects the view of the two project consortia on the consultation on the legal framework for the fundamental right to protection of personal data launched by the Commission.

Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalization

The current EU data protection legal framework is based on the 95/46/EC Directive. Since the Data Protection Directive came into force in 1995, the ways in which the personal

¹ **HIDE** (www.hideproject.org) is a project promoted by the European Commission DG Research aiming at establishing a platform devoted to monitoring the ethical and privacy implications of biometric and personal detection technologies.

² **RISE** (www.riseproject.eu) is a project promoted by the European Commission DG Research, to ensure continuity, deepen and enlarge to Asian actors the international dialogue on ethics of biometrics.



data is accessed, collected, processed, stored and used, as well as the possibilities it is abused or misused, have seen critical changes from different points of view.

1) Technological challenges

The main technological challenges are:

(a) Technology Invisibility and Miniaturization: one of the main technology trend is towards invisibility and extreme miniaturization, which is meeting an obvious request from the market and consumers. Yet this means that data subject informed consent (one of the cornerstone of current personal data protection) is increasingly hard to obtain. Subjects are often and often plunged into environments that capture and process data invisibly and unobtrusively through a vast array of embedded sensors (of many kinds, visual, acoustic, olfactory, vibratory, thermic, etc). This implies that data subject can hardly give their informed consent because they are actually unaware of what is going on. In normal situations, the data subject only appreciates the benefit of invisible technology, which is unobtrusiveness. People are hardly confronted with the downside of invisible technology, which concerns the extreme difficulty to know what data has been collected, by whom, and for what purposes. Labels or panels, which warn that the subject's personal data are invisibly collected, are a poor solution because – as various studies have demonstrated – people tend rapidly to lose awareness of these panels, which unavoidably end up going unnoticed.

(b) Smart Technology: "smart" technology means context aware, intelligent technology, which can learn from experience, take decisions, and react. Actuators react to stimuli provided by sensors, and processed by artificial intelligence. The key innovation is that sensors and actuators communicate directly with each other through invisible wireless networks, and the whole system takes decision without the need of any human direct intervention. People usually experience the benefit of smart technology, which is to create friendly, consumer tailored,



devices and environments, which recognize the data subject. Yet smart technologies imply that the data subject is going to be affected by decisions based solely on automated processing of data. This could be relatively innocuous in many situations, although never trivial (for instance in case of “smart” stores, which learn from consumer’s purchasing habits, and present tailored offers to each customer) but could turn out to be very risky when decisions concern, say, health (e.g., smart hospitals) and security (e.g., terrorist screening programs in airports).

(c) Technology Convergence: convergence between different kinds of information and communication technology (ICT convergence) and among large technology areas (ICT, Bio, Nano, Cogno) is another important trend. Convergence means, inter alia, increasing interoperability and possibility of data exchange between devices and databanks, which belong to different ICT systems, or even to different technology areas. This range from local applications (e.g., ICT body implants for medical reasons) to large scale applications (e.g., merging of biometrics and DNA data banks). One of the main impact of technology convergence on data protection is that it becomes increasingly difficult to ensure personal data traceability and transparent, public, data processing. Also other conventional data protection principles, as data limitation and proportionality, are challenged by data sharing between different technologies and devices.

2) **Globalization challenges**

The volume of data collected is expanding in terms of numbers of people affected on a global basis. Personal data is increasingly processed in an international context. The international data flows is carrying out through multinationals operating across the globe, outsourcing practices and e-commerce. The main challenges implied by globalization are:



(a) Outsourcing: Today outsourcing is often a “chain” process, in which the first ring of the chain is totally unaware of what is happening at the last ring level. Outsourcing trespasses national borders and jurisdictions, and makes increasingly difficult to ensure data traceability. Moreover, outsourcing very frequently concerns the public sector, which outsources its functions or procurement activities to the private sector. But this unavoidably implies to transfer responsibilities and authorities held by public sector entities to the private sector, which is quite arguable for many reasons. First, the private sector is often and often globalised, it means that it lies without the traditional national boundaries and jurisdiction of the public sector contractor. This implies increasing cross-jurisdictional issues. Second, free-market principles and economic incentives could result in dangerous degrees of risk-taking or compromise as to the “acceptable” costs of data loss or theft. This could be still pretty fair in case the data subject is aware of this, he consents, and he gains any benefit from risk taking, but the issue is that people are usually unaware of data outsourcing and transfer outside their natural jurisdiction, and they do not gain any special benefit.

(b) Cross-enterprise systems and applications: in parallel with outsourcing, globalization is implying another challenging trend, say, data sharing between connected enterprises and applications, which can lie both inside and outside national borders. An appalling consequence of this trend has been the creation of a huge amount of data that exists in many different forms and resides in various systems, within and outside each single organization, with an increasing difficulty to trace them. Although in principle organizations and data controllers should be able to access the data regardless of where it resides and what format it is in, this is more and more hard to be reached. As grid computing and the cloud develop, this phenomenon will be more and more apparent and critical.



(c) Cross-Jurisdiction Data Protection: traditional jurisdictional theories are based on a few principles, most of them are directly or indirectly related to the general principle of territoriality (say, a law is applicable only on acts that have been committed within the jurisdiction of the State to which a law belongs). With most ICT networks – to start with the Internet, till cloud computing –this principle is hardly applicable, and, in absence of a binding, international regulation on data protection, this means that each State applies its own legislation to the segment of the network which is under its direct control. Still the global flow of data, people, and goods tend to create various “no-man lands”, places that are suspended between different jurisdictions or even do not belong to any jurisdiction at all (think of Guantanamo). They include virtual places, like federated Internet databanks (e.g., Google), and physical spaces (e.g., airport’s transit areas, which are jurisdictional enclaves inside the territorial boundaries of a nation). The more globalization and technology progress, the more these “privacy-grey areas” will expand.

(d) Data Sharing for Forensic and Security reasons: another consequence of globalization is globalization of threats, both human made and natural. Globalization of threats implies globalization of security. After the Human Security Doctrine, launched in 2004 by the UN, the EU has adopted a similar doctrine which includes threats like conventional terrorism, bio and cyber terrorism, earthquakes, tsunamis, epidemics, an so. From the data protection perspective, this means a global drift toward merging of data collected for very disparate reasons (war against terrorism, fight to organized crime and mafia cartels, epidemiological surveillance, natural disaster preparedness, etc). Two concurrent trends are shaping this scenario. The first trend is the adoption of an intelligence-led model, in which intelligence serve as all-encompassing guide to civil protection, homeland security, public health, operations. The intelligence model



is an approach to emergency of any kind, built around risk assessment, risk management, and the extensive exploitation of a new generation of web application hybrids (*mushups*), which combine information from multiple sources into single representations. The mining power of these systems is constantly increasing. Current systems combine similar types of media, and the introduction of new automated analysis of online video materials and radio broadcasts, together with the possibility to aggregate them, is providing still more mining power. The second trend concerns the application of preventive models (originated in the medical field) to cover also homeland security and natural disaster sectors. The emphasis posed on pre-emption (of terrorism, epidemics, natural disasters, etc) relies on the increasing data storage, and handling, capacity.

In your views, the current legal framework meets these challenges?

The current EU legal framework based on the 95/46/EC Directive is only partly adequate to face up the technological, economical and political challenges to the effective protection of personal data.

On the positive side, the data protection directive sets out some strong basic principles, and provides an international reference model for good practice, giving people important and usable rights. This legal framework has helped to harmonize data protection rules across Europe and to improve the awareness of data protection concerns.

However, on the other side and on the light of the rapidly evolving challenges outlined above, the main gaps of the current EU legal framework can be summarized as follows:

- 1) Most of the definitions clearly expressed in the Directive are technologically out of date. This concerns very critical definitions, like "Personal Data" (today in many



cases it is the combination of data which renders them relatable to an “identifiable person”), “Informed Consent” (ambient intelligence and seamless communication make very difficult to apply standard procedures), and even the same notion of “Privacy” (one of the main questions with current technology is: “to what extent consumers have to be protected against their own will to provide sensitive information about themselves”).

- 2) The Directive describes a “chain process” with different degrees of authority and responsibility over the control of personal data, which is no more adequate to describe the way in which they are processed in the new technological and global scenario. The main result is that the assignation of accountability is no more evident, making difficult for individuals to exercise significant control over their personal data. The role of DPAs should also be real, and more consistent with these goals, for instance by providing guidance on how to comply with law and conducting ex post assessments on the data protection breaches.
- 3) The Data Protection Directive, focusing on principles and also procedures, used a typically European approach to the protection of personal data and a strict approach towards the international transfer of such data. This has also been pointed out as a paternalistic approach towards the implementation of the data protection principles, which doesn’t recognize that countries would have their own legislative approaches to data protection. The current system for assessing 3rd countries is too cumbersome and lengthy, and international transfer rules are unrealistic against the globalised data flows and the needs of developing economies.



What future action would be needed to address the identified challenges?

The HIDE and RISE projects consortia think that there is room for improving the EU data protection legal framework, and welcome opportunities such as this public consultation in order to strengthen the cooperation between the public and private spheres and to implement a credible data protection culture. The review of the current legal framework should take into account the following issues:

- 1) The possible redrafting of the EU data protection directive should first consider the redefinition of the object of protection, possibly using a risk-based and more flexible approach, and reviewing the weaknesses of the current bureaucratic measures. In order to assigning accountability and providing for effective enforcement, the power of intervention of DPAs should be structured as realistic and effective. In order to modernize the data export rules, the effectiveness of the adequacy rule must be improved and the use of alternatives such as SCCs and BCRs must be facilitated. The European Parliament and the European Court of Justice, as well as the national governments and regional authorities, should cooperate in this reviewing process.
- 2) The adoption of soft law instruments, able to support the introduction of best practices, ad hoc agreements and ethical codes of conduct, should be encouraged among those actors who are directly responsible for the information management and the processing of personal data.
- 3) The European Commission should continue to support the development of privacy enhancing technologies, in order to build up a sustainable and trustworthy ICT environment. Particular attention should also be given to the initiatives aiming at raising public awareness and stimulating global and multidisciplinary debate on the social, economical and technical implications related to the EU privacy and data protection legal framework.



Signed by

Aristotle University of Thessaloniki	GR	http://www.auth.gr/home/index_en.html
Biometric Research Centre HK Polytechnic University	CHINA	http://www4.comp.polyu.edu.hk/~biometrics
Centre for Biomedical Ethics, Yong Loo Lin School of Medicine	SG	http://cbme.nus.edu.sg
Centre for Policy on Emerging Technologies	US	http://www.c-pet.org
Centre for Science, Society and Citizenship (coordinator)	IT	www.cssc.eu
Centre for the Economic and Social aspects of Genomics	UK	http://www.genomicsnetwork.ac.uk/cesagen
Data Security Council of India	INDIA	http://www.dsci.in
European Biometrics Forum	IR	http://eubiometricforum.com
Eutelis Italia Srl	IT	http://www.eutelisitalia.eu/home_eng.htm
Faculty of Electrical Engineering, University of Ljubljana	SI	http://www.fe.uni-lj.si/welcome-E.html
Fraunhofer Institute for Computer Graphics Research – Dept Security Technology	DE	http://www.igd.fhg.de/igd-a8/en
Global Security Intelligence	US	http://globalseci.com/about-gsi
International Biometric Group	US	http://www.biometricgroup.com
Lancaster University	UK	http://www.lancs.ac.uk
Optel Ltd.	PL	http://www.optel.com.pl
Sagem Sécurité	FR	http://www.sagem-secureite.com
The Hastings Centre	US	http://www.thehastingscenter.org
University of Tartu	EE	http://www.ut.ee/en
Zuyd University – Infonomics & New Media Research Centre	NL	http://www.hszuyd.nl/view_subsite.jsp?content=43761