

# **Data Protection and new rights in the Digital Era**

**Giovanni BUTTARELLI**

**MEETING OF CHAIRPERSONS OF  
THE COMMITTEES SPECIALISED  
IN FUNDAMENTAL RIGHTS**

**Rome, 13 - 14 October 2014 Chamber of  
Deputies**

# Data protection and the free circulation of personal data

- EU approach is both about
  - *Protection of fundamental rights of the individuals*
  - and *ensuring free flow of data... within the EU*
  - > *Harmonisation necessary*
- Outside the EU
  - *Consumer protection*
  - *Allowing exchanges of data provided sufficient protection is afforded*



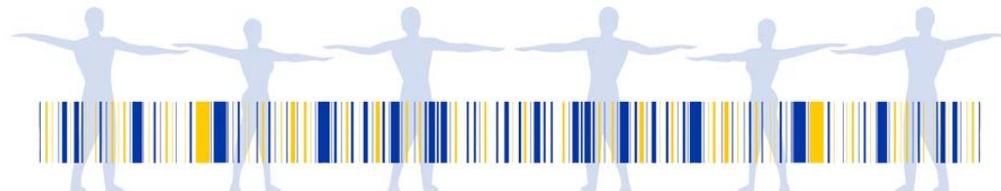


# Transborder data flows

- Possible options for lawful transfers
  - *Adequacy*
  - *Adequate safeguards*
  - *Exceptions*

Safe Harbour  
Binding Corporate Rules  
Standard Contractual  
Clauses

- Steps forward
  - *Analysis/comparison of regional approaches (BCRs-CBPRs)*  
**EU BCRs** (free flows of data between all parties to the corporate rules)  
**APEC CBPRs** (free flows of data between APEC members)
  - *Common approach to international enforcement (International Enforcement Cooperation Working Group and G-Pen)*



# International instruments

- **OECD Privacy Guidelines (2013), Part 4, point 17 and 18:** A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.
- **Modernisation of the Council of Europe Convention 108:** free transfers between parties to the Convention, unless binding harmonised rules of protection shared by States belonging to a regional international organisation. Transfers to States not Party to the Convention subject to appropriate level of personal data protection based on principles of the Convention.
- **Madrid standards, point 15:** international transfers of personal data may be carried out when the State to which such data are transmitted affords, as a minimum, the level of protection provided for in the standards. Otherwise, those who expect to transmit such data shall guarantee that the recipient will afford the same level of protection

# Other international instruments

- **GATS, art 14:** *‘Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures (...) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to (...) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.’ .*
- **Transatlantic Trade and Investment Partnership (TTIP) negotiations**
- **Budapest Convention on Cybercrime**

# How we can attain more convergence between different systems ?

- Modernisation of COE' Convention 108/1981
- Revised OECD Guidelines (2013)
- Strengthening controllers' accountability on a global scale
- Better co-operation on transborder data flows
- Stronger enforcement and cross-border enforcement co-operation networks

# **How best to ensure the interoperability of the EU rules with privacy and data protection frameworks worldwide**

*Global approach, mutual recognition or convergence of regional rules*

# **An example of interoperability: towards a common approach to enforcement**

- Convention 108 (Article 13(3): exchange of information on a Party's law and administrative practice),
- OECD Guidelines (point 21: exchange of information relating to the Guidelines, mutual assistance),
- Madrid standards (point 24(2): sharing reports, investigation techniques, communication and regulatory strategies; participating in associations, working groups, joint fora, seminars, workshops and courses, exchange of information and coordinated interventions).

# Which perspectives in the US

- US White Paper (February 2012, p. 31):

*‘ The United States is committed to engaging with its international partners to increase interoperability in privacy laws by pursuing mutual recognition, the development of codes of conduct through multistakeholder processes, and enforcement cooperation’* . Mutual recognition requires “the embrace of common values surrounding privacy and personal data protection”, as well as “effective enforcement and mechanisms that allow companies to demonstrate accountability” .

# **A New EU Data Protection Legal Framework**

## **A. The *Chapeau* Communication**

## **B. The draft Regulation**

- I. General assessment
- II. Scope, new definitions or principles
- III. Data subjects
- IV. Data controllers
- V. Supervision and enforcement
- VI. Transfer to third countries

## **C. The Directive for on police and judicial cooperation**

# *'One World, One Privacy'*

(Venice, 1990)

- A legally binding instrument valid for all countries ?
- A United Nations binding legal instrument setting out in detail the rights to data protection and privacy as enforceable human rights ?  
(2005 Montreux Declaration)
- An Additional Protocol to ICCPR ?  
(Article 17 of the International Covenant on Civil and Political Rights)  
(2013 Warsaw Resolution)
- Through an Intergovernmental Conference ?  
(2010 Jerusalem Declaration)
- International Standards ?  
(Madrid 2009)
- Universally accepted ISO privacy standards ?  
(2007 Montreal Resolution)

# *‘One World, One Privacy’*

- A broad spectrum of various solutions not necessarily alternative to each other
- Development of multi-jurisdictional arrangements to give effect to data protection principles, regardless of the personal information location

# *‘One World, One Privacy’*

- Decreasing trend in fragmenting different approaches
- Go beyond local barriers
- Building on trust and have a more common understanding
- Privacy and data protection are more and more of a global matter and need a more global response

## Reasons for a substantive Reform in the EU

- Globalisation: increased transnational flows of data to be facilitated while ensuring adequate protection
- Technological changes
- Institutional changes: the Lisbon Treaty and the Charter
- A fragmented legal framework within 28 EU Member States: need for more harmonisation and of new coherent and uniformly applied EU rules
- Legal certainty
- Need for change with regard to police and judicial activities

# **The EU DP reform:**

- A huge step forward for data protection in the EU
- Enhances harmonisation of data protection
- Reinforces position and rights of data subjects particularly on-line
- Strengthens responsibility of data controllers
- Strengthens DPA's supervision and enforcement
- lacks of full comprehensiveness

## **A window of opportunity:**

- set modern EU standards relevant for the rest of the world

# Territorial scope and conflict of laws at international level

Controllers or processors established within EU

Non EU-based data controllers: *‘offering goods and services to’* or *‘monitoring behaviour of’* data subjects in the EU

Art. 43a of the draft Regulation and surveillance activities by third countries law enforcement bodies

# Three main challenges

**Regulation and national laws: which level of harmonisation ?:**

- a) national legislation needs to be repealed;
- b) margins for manouvre for MS (in principle: no additions allowed under national law but...);
- c) which national laws;
- d) the national acquis on non-data protection areas

**New neutral approaches to be stable in the mid-term, to make them fit for the 21st century: Internet as electricity**

**Anticipate the Big Data World we will inhabit until 2025**

# Big Data

- Not only a data protection issue
- 'Seizing opportunities, preserving values'*
- significant benefits, prosperity, well-being
- discrimination and surveillance
- a new challenge for data protection, but not a fundamental one: it requires innovative thinking
- the ethical dimension

# Big Data

- -effective technology-proof rules
- -notice and choice
- -who will be in control and of what
- -profiling: a new notion of harm ?
- -the value of dispersed data
- -a new concept of identifiability ?
- -re-identification techniques ?
- -which quality of data
- -need to know principle, retention time limits
- -co-data subjects ?

# Big Data

- Should data principles and obligations under EU law be substantially reviewed because of Big Data ?
- The current EU package may help a great deal: the robust and right approach we need
- Existing principles continue to be valid
- New, innovative and practical ways to successfully apply them in practice
- Ensure we are not surprised by rapid developments
- A European Digital Habeas Corpus ? (EP, 2013)
- Data as today's currency, a nuclear weapon: results will be relevant for the asset of democratic countries

# Thank you for your attention



[@EU\\_EDPS](https://twitter.com/EU_EDPS)

