

# *EU data protection view on the Internet of Things: the EDPS experience*

## Legal Notice:

*The view expressed in these slides presents the results of researches conducted by the author and his colleagues. It does not necessarily reflect those of the European Data Protection Supervisor.*

# Overview

- EU fundamental rights in a nutshell
- Concept of Internet of things
- Privacy and Data protection concerns
- Implementation of Data Protection principles and safeguards
- Involvement of the EDPS
- Roles of the EDPS
- EDPS cases

# EU fundamental rights

## Respect for private life(Article 7 EU Charter)

- Provided by law
- Legitimate purpose
- Necessity & proportionality
- Adequate safeguards

## Protection of personal data(Article 8 EU Charter)

- Lawful processing
- Purpose limitation
- Data quality
- Transparency
- Rights of data subject

# Internet of Things (IOT): concept

- Awareness of the world
- Serves for:
  - Identity of things
  - Integration of objects into the digital world
    - Connection between objects
    - Interaction with users
- Other definitions (IOT Communication)



EUROPEAN DATA  
PROTECTION SUPERVISOR

# Internet of Things (IOT)



European Data Protection Supervisor

- Scope of concept is often misunderstood:
  - Not only RFID
  - Not only RFID, sensors, readers
- Covers interactions between RFID, sensors, readers, Internet protocol, wireless interfaces and processing operations

# Functionalities

- Localisation
- Identification
- Processing
- Sensing
- Communication between and through objects
- Context-aware applications

The concept itself and its applications are, in principle, very promising to foster the Information Society but...



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Privacy/data protection concerns

European Data Protection Supervisor

- Personal Data stored in tags or connected to Personal data eavesdropping risks
- Profiling
- Tracking of users without their knowledge
- Data processing everywhere
- Information technology becomes invisible



EUROPEAN DATA  
PROTECTION SUPERVISOR

# Data Protection principles apply to the IOT



European Data Protection Supervisor

- Purpose limitation
- Proportionality
- Necessity
- Data minimization
- Transparent data retention
- Security
- Information
- Responsibility & Accountability



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Implementing Privacy and Data Protection safeguards

European Data Protection Supervisor

- Derived from Existing Data Protection Framework:
  - General Data Protection Directive 95/46
  - E-Privacy Directive 2002/58 (under revision)
  - RFID Recommendation



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Implementing Privacy and Data Protection safeguards

European Data Protection Supervisor

- Privacy and Data Protection Impact assessments
- Security Impact assessments
- Privacy by Design
- Best Available Techniques for Security and Accountability

# Necessity for new legislation?

- Legislator provides for the legal framework
- In principle, clear need for guidance and interpretation of the application of existing legislation
- Depending on the effectiveness of the above, it is not excluded that better implementation or additional legislation may be necessary.



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Quick overview on the Legal Framework of the EDPS

- Article 286 of EC Treaty
  - Community acts on the protection of individuals with regard to the processing of personal data and free movement of such data shall apply to Community institutions
  - Establishment of an independent supervisory authority
- Directive 95/46/EC + 2002/58/EC (under revision)
- Adoption of Regulation (EC) N° 45/2001
  - Entry into force January 2001
- Decision 22 December 2003 appointing EDPS and Assistant
- Since 17 January 2009, new Assistant EDPS



EUROPEAN DATA  
PROTECTION SUPERVISOR



## Roles of EDPS

- Supervision
  - Prior checks of processing operations in the EU Institutions: Access controls, Flexitime
  - Inspections and audits
- Consultation
  - Opinions on RFID, EU passport
  - Evaluation of FP7 research projects
- Cooperation
  - Opinions of Article 29 Working Party (Member)

# Involvement of the EDPS on RFID matters

- Technology subgroup of Article 29
- Observer RFID expert group
- Follows RFID Recommendation (May)
- Follows IoT Communication (June)
- Follows Research projects in 7<sup>th</sup> Framework Programme

# Supervision

- Task of EDPS is to monitor and ensure that the provisions of Regulation (EC) No 45/2001, as well as other Community acts on the protection of fundamental rights and freedoms, are complied with when EU institutions and bodies process personal data;
- Mostly supervising RFID applications: An RFID tag is an object that can be applied to or incorporated into a product, an animal or a person for the purpose of identification or remote tracking through the use of radio waves. (EDPS glossary)



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Why supervising RFID implementation?

European Data Protection Supervisor

- In the analysed cases, the identification number associated to the RFID chip is personal data covered by Regulation 45/2001
- Political reason

## Specific prior-checking cases (i) Recording by RFID badge for Flexitime

- Flexitime is designed to enable staff to achieve a better balance between their private and professional life
- Flexitime is also designed to enable the institutions to manage attendance more effectively in accordance with work requirements
- In this way, institutions intend to increase the motivation of their staff by making them more responsible for organising their working time.
- Implementation of RFID badges to clock in and out: the inclusion of RFID technology in the badge of the flexitime system brings specific risks in the system



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Recommendations

European Data Protection Supervisor

- There is not a specific need to develop a badging system using RFID to implement a flexitime system but there is a margin of appreciation left at the discretion of the administration in deciding to implement a system using RFID.
- Choice of technology based on best available techniques (cloning, tracking).
- Set the reading distance to its minimum.
- Limit the recipients of the data to the concerned persons (i.e. not to the local security officer)

## **Specific prior-checking cases (ii)**

### **Recording by RFID badge for access control**

- Implementation of RFID badges for Identity and Access Control System to ensure that only authorised persons have access outside working hours and special secure zones. To do so, there is use of a smartcard and fingerprint authentication. Users' biometrics data are stored only on the smartcard which cannot be used for any other purpose.



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Recommendations

European Data Protection Supervisor

- Integrate privacy/data protection considerations in future impact assessment
- to reconsider the technological system taking into account the choice of the best available techniques and discussions on future security systems. Biometric data (additional risks)

# Consultation

- Task of the EDPS to advise the EU institutions and bodies on all matters relating to the processing of personal data; this includes consultation on proposals for legislation and monitoring new developments that have an impact on the protection of personal data

## **Opinion on Communication on RFID in Europe: steps towards a policy framework**

- Opinion of 17 December 2007
- RFID systems could play a key role in the development of the European information society, but also the wide acceptance of RFID technologies should be facilitated by the benefits of consistent data protection safeguards.
- It is appropriate in the first phase to leave room for self-regulatory instruments but additional specific legislative measures may be necessary to regulate RFID usage in relation to privacy and data protection.

# Recommendations

- The provision of a clear guidance, in close cooperation with relevant stakeholders, on how to apply the current legal framework to the RFID environment;
- The adoption of Community legislation regulating the main issues of RFID usage in case the effective implementation of the existing legal framework fails;
- Such measures should notably lay down the opt-in principle at the point of sale as a precise and undeniable legal obligation;
- The identification of ‘best available techniques’ which will play a decisive role in the early adoption of the privacy-by-design principle.

# Cooperation

- Task of EDPS to cooperate with national supervisory authorities and supervisory bodies in the ‘third pillar’ of the EU with a view to improving consistency in the protection of personal data
- Observer in the Expert Group on Radio Frequency Identification/RFID-Stakeholders Group
- Article 29 Data Protection Working Party:
  - Opinion No 4/2007 on the concept of personal data (2008)
  - Working document on data protection issues related to RFID technology (2005)



EUROPEAN DATA  
PROTECTION SUPERVISOR



European Data Protection Supervisor



**THANK YOU!!!**

**More information:**

[www.edps.europa.eu](http://www.edps.europa.eu)

**Contacts:**

[edps@edps.europa.eu](mailto:edps@edps.europa.eu)

[michael.vanfleteren@edps.europa.eu](mailto:michael.vanfleteren@edps.europa.eu)

Postal address:

Rue Wiertz 60 - MO 63

B-1047 Brussels