



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Cloud Computing: Privacy Risks and EU Policy Considerations

Rosa Barcelo

Legal adviser

European Data Protection Supervisor

The Future of Cloud Computing, 26 January 2010 Brussels



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Overview

- Privacy risks in a nutshell
- Application of EU data protection legislation
- Challenges & gaps in EU data protection legislation
- Conclusions

The Future of Cloud Computing, 26 January 2010 Brussels



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Privacy risks in a nutshell

The Future of Cloud Computing, 26 January 2010 Brussels



EUROPEAN DATA
PROTECTION SUPERVISOR

Privacy risks in a nutshell I

- Cloud computing from a privacy perspective:
 - Many cloud applications for consumers
 - Personal photos, calendars, on-line hard drive backups
 - Terabytes of data (some sensitive)
 - “all I want to know about you”
 - Also the log files accessing the cloud
 - Stored in centres around the world



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Privacy risks in a nutshell II

- Risks to individuals' privacy.
Examples:
 - Security glitches (unintended)
 - Hacking (recent Google case in China)



EUROPEAN DATA
PROTECTION SUPERVISOR

Privacy risks in a nutshell II

- Risks to individuals' privacy.
Examples (cont):
 - Risk of use of data for unrelated purposes
 - Accessibility restrictions (losing control)
 - Data stored in countries with poor data protection laws
 - Wiretapping by Governments

Privacy risks in a nutshell III

- Coping with the personal data/privacy risks:
 - US approach
 - EU:
 - Data protection Directive
 - Eprivacy Directive



European Data Protection Supervisor

Application of EU data protection legislation

The Future of Cloud Computing, 26 January 2010 Brussels



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Application of EU data protection legislation I

- If Directives apply, cloud provider must (if it is “controller”) ensure compliance:
 - Ensure the security of the data and subsequent responsibility (Art 17)
 - Provide information to individuals (Art 10)



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Application of EU data protection legislation II

- Application of the purpose limitation principle (Article 6)
- Restriction on international data transfers (Arts 25 and 26)



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Application of EU data protection legislation III

- Responsibilities if cloud computing provider fails to fulfill its obligations
- Authorities have enforcement powers

The Future of Cloud Computing, 26 January 2010 Brussels



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

Challenges and gaps in EU data protection legislation

The Future of Cloud Computing, 26 January 2010 Brussels



The Challenges I

- Is the cloud provider a data controller or a processor?
 - The responsibilities are different;
 - Probably, processor but it will depend on the circumstances;
 - BUT, remember SWIFT case; increasingly deemed ‘joint controllers’ with different responsibilities;
 - WP 29 Guidance



The Challenges II

- Determining whether the Directives apply:
 - Controller is established in the EU
 - Controller not established in the EU but uses equipment located in the EU for the processing of personal data

Social networks, search engines: WP 29 opinions
(this issue is not new)



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

The Challenges II

- Determining whether the Directives apply:
 - If controller targets services to EU but does not use equipment within and is not established within EU: no application (Art. 25 applies)



EUROPEAN DATA
PROTECTION SUPERVISOR

The Challenges & Gaps III

- If cloud client is an individual using the cloud for private purposes (eg calendar, storing pictures):
 - Similar to Picasa;
 - Does the Directive apply at all? Is there a *lacuna* and thus a lack of protection?
 - What are the responsibilities of the cloud provider in such cases?

The Challenges IV

- Compliance with provisions on international data transfers:
 - Is it a data transfer? (Bodil Lindqvist)
 - Notification to authorities
 - Safe Harbour and adequacy findings
 - Putting contracts in place
 - BCRs & others
- Difficult for multiple transfers which are often the case



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

The Challenges V

- Compliance with transparency provisions vis-a-vis individuals:
 - Ensure that consumers know about the location of their data
 - Ensure that they properly understand the risks so that they can make informed choices



EUROPEAN DATA
PROTECTION SUPERVISOR

European Data Protection Supervisor

The Challenges V

- The challenges are not new:
 - Similar challenges have been present since the Internet began
- Cloud computing simply **INTENSIFIES** them

The Future of Cloud Computing, 26 January 2010 Brussels

Conclusions I

- How to address the Challenges & Gaps?
 - Probably not one single magic solution but a combination of solutions
 - Need to do “homework” to find solutions
 - Solutions may be part of broader attempt to solve other (wider) problems

Conclusions II

- Solutions & Venues to solve challenges/gaps:
 - Technology solutions: Privacy by Design - take into account data protection when designing cloud computing services
 - Interpretation and Guidance: Court & WP 29

Conclusions III

- Solutions & Venues to solve challenges/gaps (cont):
 - Current review process of the existing Data Protection Directive:
 - Criteria for applicable law (targeting);
 - New principles: Privacy by design, accountability
 - Data controller/processor: Hybrids; new category necessary? Responsibilities should be attached to each category (security obligations)
 - Updated rules on international data transfers

Questions?