An integrated privacy and ethical impact assessment

David Wright
Managing Partner
Trilateral Research & Consulting
at the PRECIENT conference
Berlin
28 November 2012
Definition of PIA

• A process for assessing the impacts on privacy of a project, technology, service, policy or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts

• A PIA is about identifying risks and finding solutions, not simply producing a report that demonstrates compliance
Definition of an EIA

• A process for identifying, examining and assessing the ethical issues arising from the development of a project, technology, service, policy or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts.

• An EIA process is similar to that of a PIA. The major difference is that a wider range of issues may need to be examined and a wider range of stakeholders (e.g., ethicists, sociologists) consulted.
Article 33

- Obliges data controllers to carry out a “data protection impact assessment” where processing presents “specific risks to the rights and freedoms of data subjects”

Art. 33(2) cites examples of such risks:
- a systematic and extensive evaluation of a person's economic situation, location, health, personal preferences, reliability or behaviour
- information on sex life, health, race and ethnic origin
- video surveillance
- genetic or biometric data
- other processing operations requiring consultation with the DPA
Art. 33 (3) describes what the assessment shall contain:
- a description of the envisaged processing operations,
- an assessment of the risks
- measures to address the risks
- safeguards to ensure protection of personal data
- compliance with this Regulation

Art. 33 (4) -- The controller shall seek the views of data subjects

Art. 33 would empower the EC to adopt “delegated acts” re verifying and auditing the assessment
A step-by-step guide to P+EIA (1)

1. Determine whether a P+EIA is necessary (threshold analysis)
2. Identify the P+EIA team and set the team’s terms of reference, resources and time frame
3. Prepare a P+EIA plan
4. Determine the budget for the P+EIA
5. Describe the proposed project to be assessed
6. Identify stakeholders
7. Analyse the information flows, privacy and ethical impacts
8. Consult with stakeholders
A step-by-step guide to P+EIA (2)

9. Check the project complies with legislation
10. Identify risks and possible solutions
11. Formulate recommendations
12. Prepare and publish the report, e.g., on the organisation’s website
13. Implement the recommendations
14. Third-party review and/or audit of the P+EIA
15. Update the P+EIA if there are changes in the project
16. Embed privacy awareness and ethical sensitivity throughout the organisation and ensure accountability
Ethical issues

• Autonomy
• Dignity
• Informed consent
• Trust
• Fairness
• Security
• Responsibility
• Harm
• Justice (right of inspection and redress)
• Solidarity and benefit sharing
• and/or others
Benefits of P+EIA

• An early warning system, a way to detect privacy and ethical problems, build safeguards before, not after, heavy investment – Fix privacy problems and ethical issues now, not later
• Avoids costly or embarrassing mistakes
• Provides evidence that an organisation attempted to prevent privacy risks and deal with ethical issues (reduce liability, negative publicity, damage to reputation)
• Enhances informed decision-making
• A way to gain the public’s trust and confidence
• Demonstrates to employees, contractors, customers, citizens that the organisation takes privacy, ethics seriously
Further reading