



Privacy Impact Assessment Handbook

Privacy Impact Assessment Project



This presentation

1. Development

- International and UK context
- Methodology

2. The Handbook

- Key features
- Feedback

3. Conclusions

- A tool for guidance



Project team

- Professor Charles Oppenheim, Dr Adam Warren – Loughborough University
- Dr Roger Clarke - Xamax Consultancy Pty Ltd, Canberra, Australia
- Robin Bayley – Linden Consulting Inc, Canada
- Professor Colin Bennett – Linden Consulting Inc, Canada
- Andrew Charlesworth - Bristol University

➡ International expertise; strong track record in privacy, legal and public policy, business processes...



International context

- 'A systematic risk assessment tool that can be usefully integrated into decision-making processes'
- PIAs conducted in a number of countries incl Canada (and provinces), Australia, New Zealand and United States
- Various tools: handbooks, eLearning tools
- Notable handbooks:
 - Australian Privacy Commissioner (2006)
 - New Zealand Privacy Commissioner (2002)
 - Ontario Management Board Secretariat (2001)
- Another option:
 - eLearning Tool (Canada, 2003)
http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a_e.asp



UK context

- First PIA exercise in the UK
 - No formal Parliamentary backing
 - Some work in this field:
 - Northern Ireland Valuation and Lands Agency
 - Multinationals
 - Integrated within existing business processes:
 - IT procurement policy
 - 'Threat risk' assessments
 - Reputation management
- ➡ OGC Gateway Review Process for Programmes and Projects



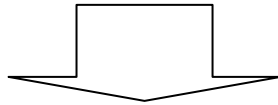
Methodology

- 'As simple as practicable, but as complex as necessary'
- Single form of PIA not adequate:
 - Degree of risk varies
 - Projects vary
 - Multiple forms of PIA likely to confuse, but Handbook must not look like a 'weighty tome'...
- Therefore...
 1. Use of PIA Screening Tool
 - Organisations diverted into the right streams
 2. Present as tiered website
 - Each organisation views sections that are relevant to it
 - PDF version that consolidates all the elements

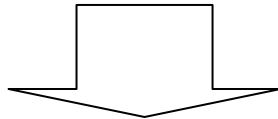


PIA Screening Tool

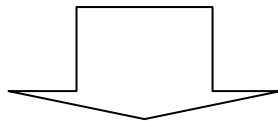
STEP 1 – Is a Full Scale PIA necessary?



STEP 2 – Is a Small Scale PIA necessary?



STEP 3 – Is Privacy Law Compliance Checking necessary?



STEP 4 – Is Data Protection Act Compliance Checking necessary?



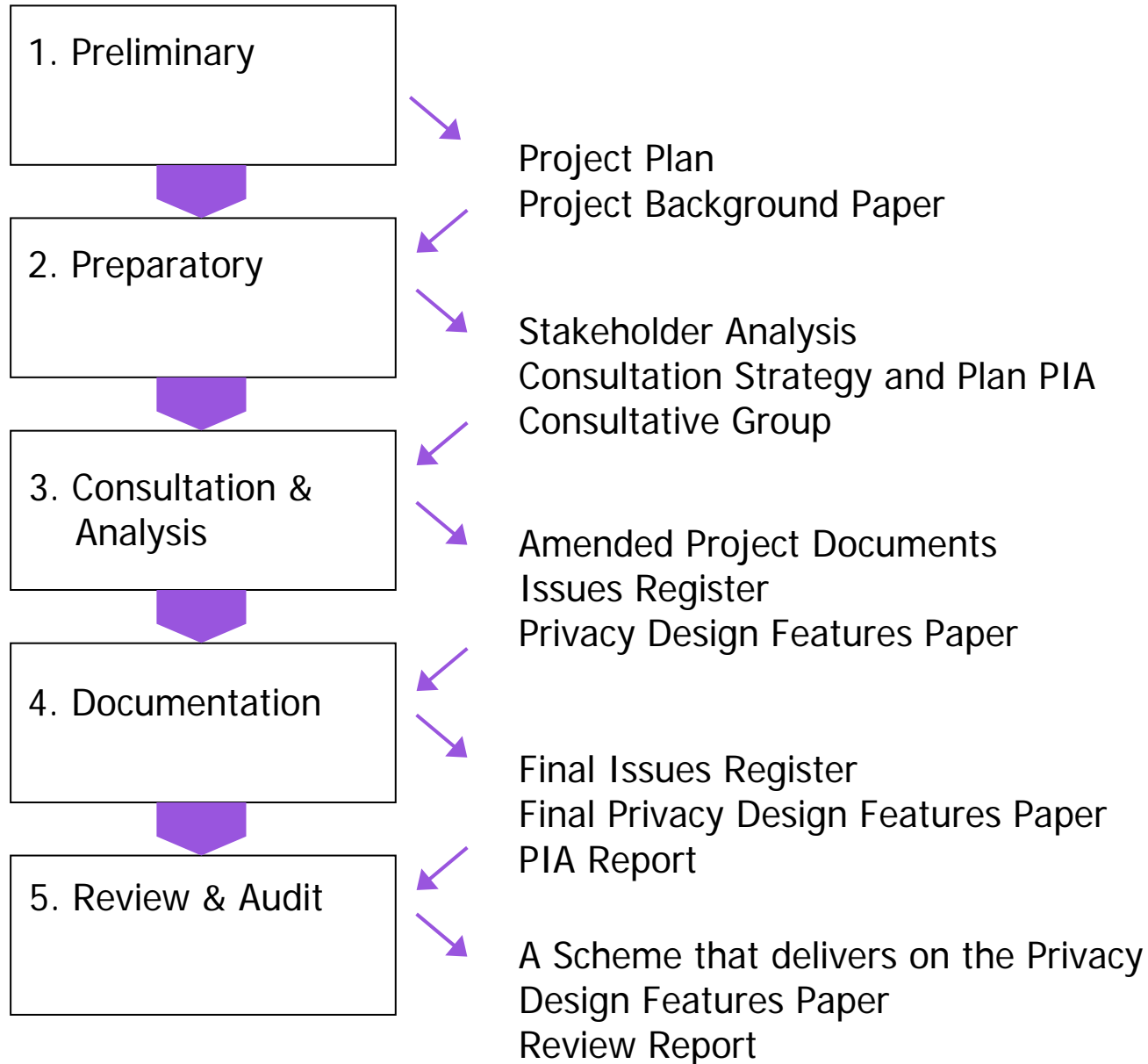
Full Scale PIA - scenarios

Projects that have considerable implications for privacy:

- Application of new or additional information technologies, entailing substantial potential for privacy invasiveness;
- Use of new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes;
- Multiple organisations, i.e. government agencies (e.g. 'joined-up government' initiatives) or private sector organisations (e.g. outsourced service providers or 'business partners');
- New or significantly changed handling of personal data that is of particular concern to people;
- Data handling which is in any way exempt from legislative privacy protections.

Phases

Deliverables





Full Scale PIA – Phases 1-2

1. Preliminary Phase

- Project Plan
- Project Background Paper
 - Establish basis for discussions with stakeholders

2. Preparatory Phase

- Stakeholder Analysis
 - Ensure major players identified
- Consultation Strategy
 - Ensure discussions with stakeholders effective
- PIA Consultative Group
 - Include relevant stakeholder groups



Full Scale PIA – Phases 3-5

3. Consultation and Analysis Phase(s)

- Amended Project Documents
- Issues Register
 - Record of privacy issues identified
- Privacy Design Features Paper
 - Features designed to address privacy issues

4. Documentation Phase

- Final Issues Register
- Final Privacy Design Features Paper
- PIA Report

5. Review and Audit Phase

- A scheme that delivers on Privacy Design Features Paper
- Review Report



Small Scale PIA - scenarios

Projects whose implications for privacy are specific rather than highly intensive

- Introduction of security cards for staff to control entry to buildings
- Addition of further data item to an existing database
- Application of a new technology to an existing purpose
- Plans to outsource business processes involving personal data, or the storage and processing of personal data
- Application of existing personal data to a new purpose
- Use of head-mounted cameras for prevention fly-tipping
- Introduction of cameras on fishing vessels



Small Scale PIA - process

- Differs from Full Scale PIA:
 - Less formalised
 - Involves less investment
 - Calls for less exhaustive analysis and information-gathering
 - Is more likely to be focused on specific aspects of the project rather than the project as a whole
- The process
 - Can be more highly structured
 - Can be delegated to less senior staff, although executive oversight still required
 - Can use the same phase structure as Full Scale PIA, but is much briefer



Compliance Checks

1. **'Privacy law'**: check that laws other than the Data Protection Act are relevant e.g.
 - Law of confidence
 - Torts of negligence, passing off
 - Provisions within statutes relating to public health, education, family law etc
 - Govt agencies: provisions within the statutes that govern their activities and programmes
 - Emerging tort of privacy?

Specific example of delegated privacy legislation: Privacy and Electronic Communications Regulations 2003
2. **Data Protection**: establish whether the provisions of the Data Protection Act are applicable



Privacy Law Compliance Check

Step 3 of the Screening Process. Key questions:

1. Does the project involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or secondary legislation, other than the Data Protection Act?
2. Does the project involve any activities (including any data handling) that are subject to **common law constraints relevant to privacy**?
3. Does the project involve any activities (including any data handling) that are subject to **less formal requirements relevant to privacy**?

Template: PECR Direct Marketing Compliance Check



DPA Compliance Check

Step 4 of the Screening Process. Two questions:

1. Does the project involve the handling of any data that is **personal data, as that term is used in the Data Protection Act?**
2. Even if the organisation claims that the project is covered by one of the limited forms of exemption and exception available under the Act, **does the organisation have a policy position of taking the Data Protection Principles into account?**

Template: Data Protection Compliance Check



Feedback: focus group #1

- 'Road-testing' unrealistic within 16 week project timeframe, but need for practitioner feedback
- Focus group
 - 12 reps from central govt, local govt and private sector with considerable experience of DP and project dvlpt at senior level
 - One third engaged in some form of 'PIA process', which they found valuable in terms of management decision-making and part of threat-risk assessment process

➡ Support for guidance in methods of incorporating PIA into existing business/management processes – e.g. in the public sector, the OGC Gateway Review for Programmes & Projects



Feedback: focus group #2

- Concerns

- 'Too resource-intensive'
- 'Trying to do too much'?

- Requirements

- Use cases that outlined the benefits of PIA processes and demonstrated where they might best fit within organisation's business processes
- Tools that were customisable to different business environments / that were designed for particular business environments
- Tools that would help focus and clarify questions about projects, services and other developments to the ICO
- ICO to work to harmonise its PIA guidance with, or embed it within, current project management processes such as the OGC's Gateway process



Conclusions

- First time PIAs been conducted in UK – breaks new ground
- A flexible, dynamic tool:
 - Web, disc and PDF versions
- Benefited from our research
- Lays the foundation for future variants. Could be developed in a number of ways:
 - Mini-case studies / vignettes
 - Bespoke guidance for small projects
 - e-learning tool – accessible courses in management, coordination and review of PIAs



Practitioners use it and provide feedback to ICO over 12 month period