

The ICO Privacy impact assessment handbook

A workshop on the ICO model for PIA

Stephen McCartney, Head of DP Promotion



ICO Privacy Impact Assessment Handbook

- Launched 11 December 2007
- First handbook for PIA in UK
- Part of the ICO “surveillance society” strategy
- International study of PIAs
- Based on practice in other countries e.g. Canada, Australia
- ICO promoting use of PIAs within government and private sector

Know the dangers ahead!



© NATIONAL NEWS

Why a PIA handbook?

The ICO envisage the handbook providing a process which:

- helps organisations consider privacy risks to individuals;
- wider than data protection;
- started at an early stage of a project;
- enables organisations to:
 - foresee problems;
 - identify solutions; and
 - create privacy friendly culture in organisation.

When do you start a PIA?

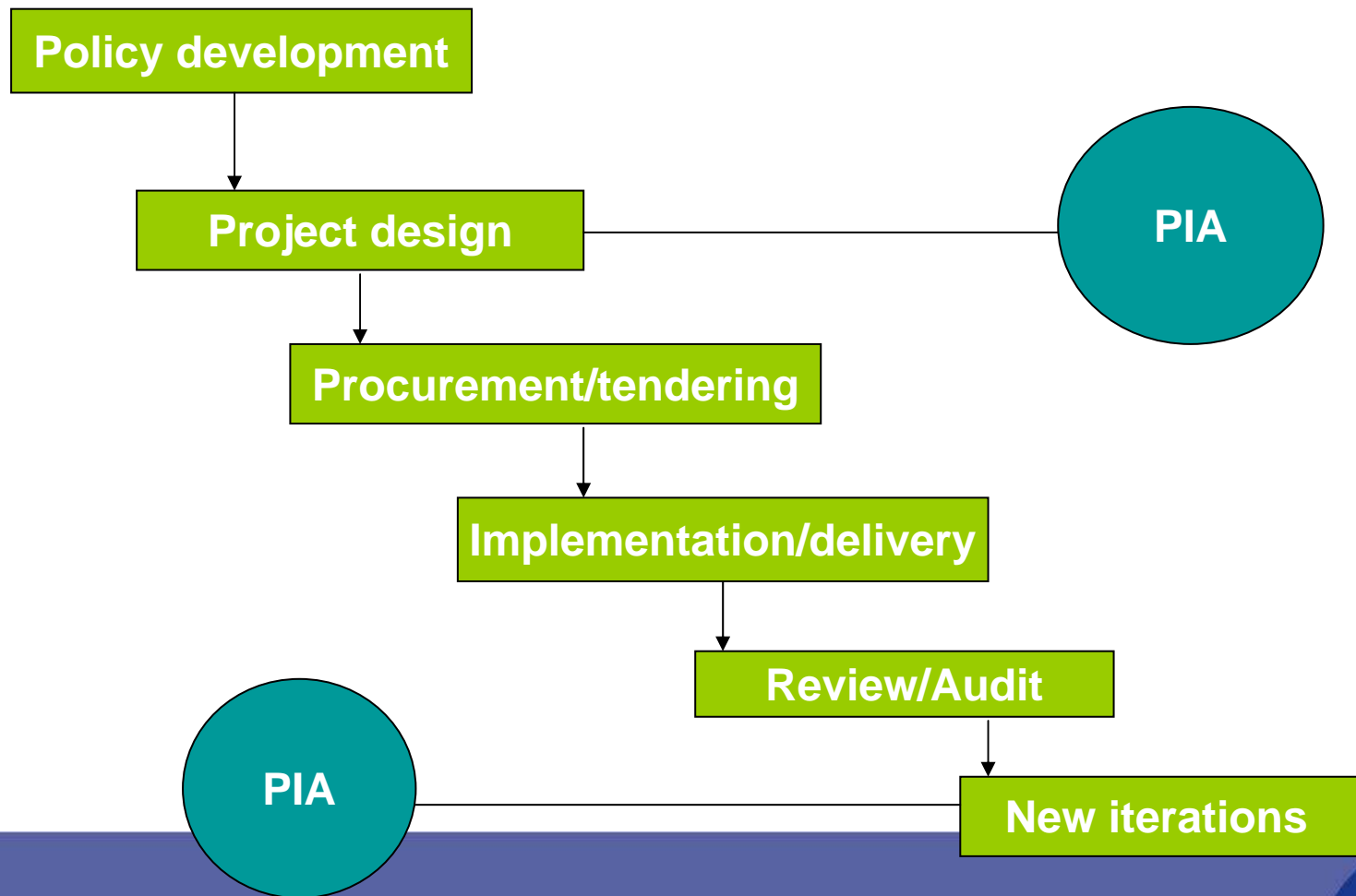
When:

- the project is being designed;
- you know what you want to do;
- you know how you want to do it; and
- you know who else you want to be involved.

But before:

- decisions are set in stone;
- you have procured systems;
- you have signed agreements/given undertakings; and
- you can still change your mind!

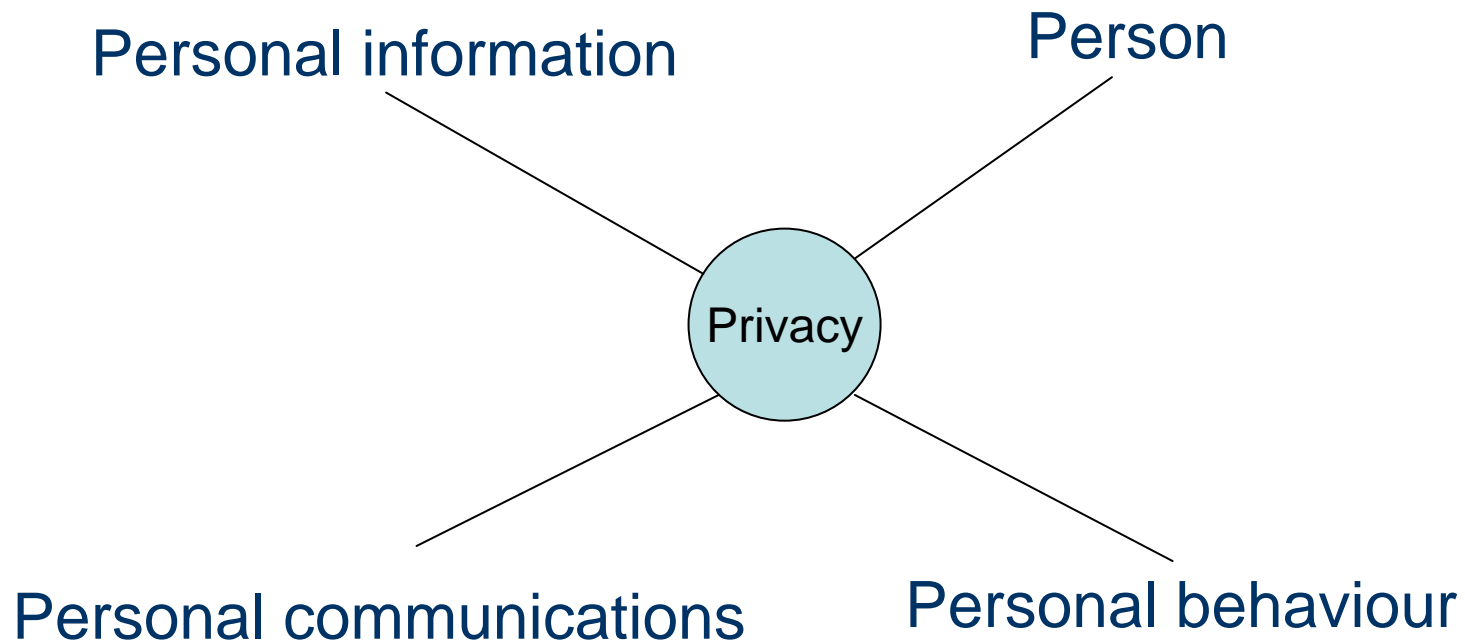
PIAs in the life cycle of a project



Why do a PIA?

- Identify and mitigate risks
- Reputation
- Public trust and confidence
- Avoid expensive “bolt on” solutions
- Cabinet Office requirement for Central Govt.
- Enlightened self-interest

Wider than data protection



The ICO model of PIA

- Initial assessment
- Full scale or small scale PIA?
- Legal compliance check
 - Privacy law
 - Statutory powers and prohibitions
- Data protection compliance check

Initial assessment

- Prepare a project outline
- Identify stakeholders
- Look at other PIAs
- Look at studies on the technology/processes
- Decide on which level of assessment is required

Full scale PIA

5 phases:

- Preliminary work
- Preparation
- Consultation/analysis
- Conclusions
- Review

Small scale PIA

Similar considerations to full-scale PIA, but

- it is less formalised;
- it involves less investment;
- it calls for less exhaustive analysis and information-gathering, and
- it is more likely to be focused on specific aspects of the project rather than the project as a whole.

Privacy law compliance check

- Narrower focus on legal compliance
- Examine relevant privacy laws
- Consider organisation's powers
- Consider legal obligations
- Statutory prohibitions
- HRA, PECR, DPA, law of confidence

Data protection compliance check

- Checklist for compliance with DPA
- Done as part of each level of PIA
- Straightforward
- Normally considered later in process, when project is more fully formed
- Considers the DP principles, conditions and exemptions

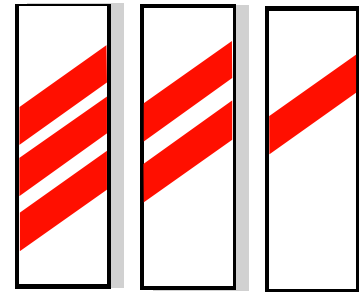
Privacy risks

Once you have identified the risks to privacy you have to make some decisions:

- Do you accept the risks?
- Do you mitigate/ameliorate the risks?
- Do you propose a less privacy intrusive course of action?

How do you mitigate risks?

- Privacy impact avoidance measures
- Privacy impact reduction measures
- Privacy enhancing technologies



Key points to remember

- PIAs are a PROCESS to consider privacy risks
- Not every use of personal information will require a PIA
- Not just for the virtuous
- Does not need to be done as a separate exercise
- ICO are here to help and advise on PIAs

Remember why you do a PIA!



Questions?

For further information contact:

**Information Commissioner's Office
Wycliffe House, Water Lane,
Wilmslow, SK9 5AF**

**Switchboard: 01625 545 700
Helpline: 01625 545 745**

Email. stephen.mccartney@ico.gsi.gov.uk

www.ico.gov.uk

And finally.....

Your chance to comment!

Give us some feedback on PIAs

- Questions
- Comments
- Praise
- Criticism

