

Privacy by design

Judith Jones

Data Protection Development Manager

Information Commissioner's Office

2 December 2009

ICO Privacy by Design Initiative

- Increasing amounts of personal information, increasing risks to individuals
- Technology used in innovative ways to exploit personal information but not always to protect it
- Technological and procedural safeguards have lagged behind
- Better to build in protection rather than bolt on

2

What is privacy by design?

- Building privacy and data protection into information systems and processes from the very start and throughout the lifecycle. This approach:
 - considers privacy prior to the development of any new system or process
 - maintains control throughout system's lifecycle, from the earliest stages of developing a business case, through to decommissioning.

3

ICO Privacy By Design Work

- Building in not bolting on
- Tools to help:
 - Privacy Impact Assessment Handbook
 - Explaining different forms of ID management
 - Promoting privacy enhancing technologies
 - Codes of practice/guidance
 - Information assurance
 - Information governance
- Privacy by Design report commissioned from Enterprise Privacy Group, launched 26 November 2008

4

Privacy by Design Report - EPG

- Barriers
- Delivery
- Comparison with 'Security by Design'
- Engaging with executive level
- Planning-PIAs
- Sharing Personal Information
- Privacy Standards
- Privacy Enhancing Technologies
- Compliance and Regulation

5

Barriers to privacy by design

- poor executive awareness and a failure to recognise privacy duties at the highest levels
- lack of consideration for privacy needs throughout the systems lifecycle
- conflicting pressures between privacy and data sharing within and outside of organisations
- lack of internationally recognised privacy management standards
- poor understanding and adoption of PETs
- need for a stronger, better funded ICO

6

Engaging with executive management

- Ensure executive managers understand their privacy duties, communicate privacy needs clearly, and demand Privacy Impact Assessments (PIAs) in system business cases
 - create a popular mandate for Privacy by Design
 - demonstrate business benefits, costs and risks of failing to comply with privacy requirements
 - create and promote a simple, shared language for discussing privacy concepts

7

Planning for Privacy by Design

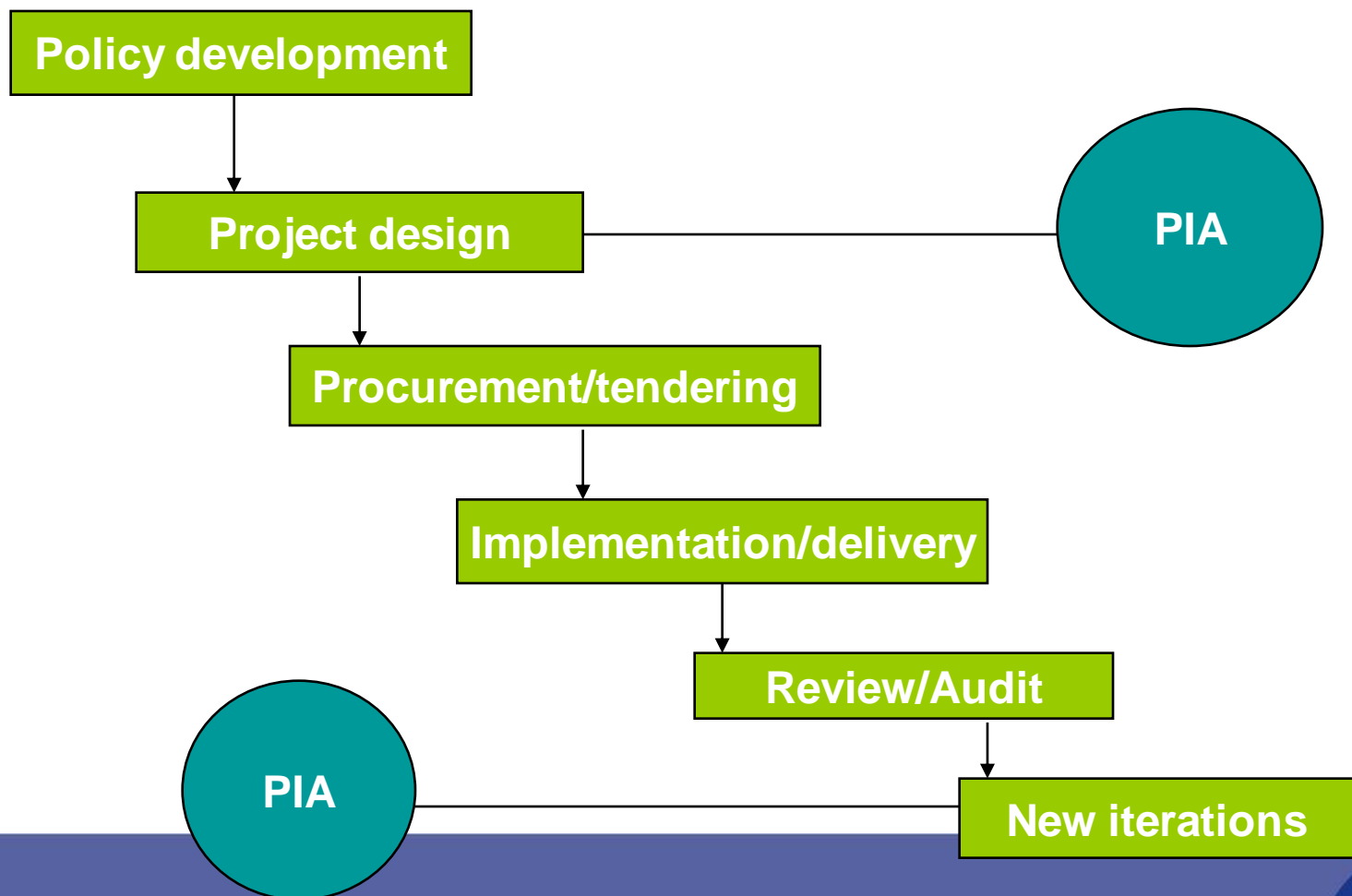
- Ensure all systems incorporate appropriate PETs based upon a PIA, and that this is managed throughout the systems lifecycle
 - make the PIA a mandatory managed document as part of the systems lifecycle
 - submit PIAs for the most sensitive systems to the ICO for verification
 - promote transparency by publishing PIAs
 - ensure that all relevant systems incorporate automated Subject Access Request functionality

Promoting PETs

- Encourage vendors to incorporate PETs into their products, and organisations to recognise the value of using those products
 - organisations demand privacy functionality as a 'deal breaker' in systems procurement
 - systems incorporate PETs, particularly for minimisation, revocation and deletion of data
 - experts develop approaches to audit and prove privacy functionality of systems
 - government supports development of commercial PETs

9

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 England Central Government
- Informs project media strategy
- Enlightened self-interest

11

ICO PIA handbook Version 2.0

- New, simpler structure
 - Discussion on privacy
 - ‘How to’ section
 - Templates
 - Process maps
- Designed mainly for online use
- Printable version off page one of html

12

Privacy enhancing technologies

- Encryption
- Biometrics
- Anonymisation and pseudonymisation
- Securely managing logins and passwords
- Restrict traceability and limit surveillance
- Secure online access for individuals to check accuracy and make amendments 13

Case studies

- Development and use of an accountability tool - holistic approach to privacy
- Remote health care system with many privacy features
- Encrypted biometric access system that allows use of a fingerprint to authenticate an identity but does not retain the information

14

Developments

- New powers and penalties for the ICO so it can investigate and enforce compliance
- New ICO research project – the business and economic case for proactive privacy protection
- New ICO code of practice – personal information on-line. Conference to launch consultation in December 2009
- European Commission's study on the economic benefits of PETs

15

Further information

- ICO website - privacy by design quicklink
http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx
- Information and Privacy Commissioner Ontario
<http://www.privacybydesign.ca/>



Information Commissioner's Office

www.ico.gov.uk