

# The Year Ahead: ICO DP Initiatives

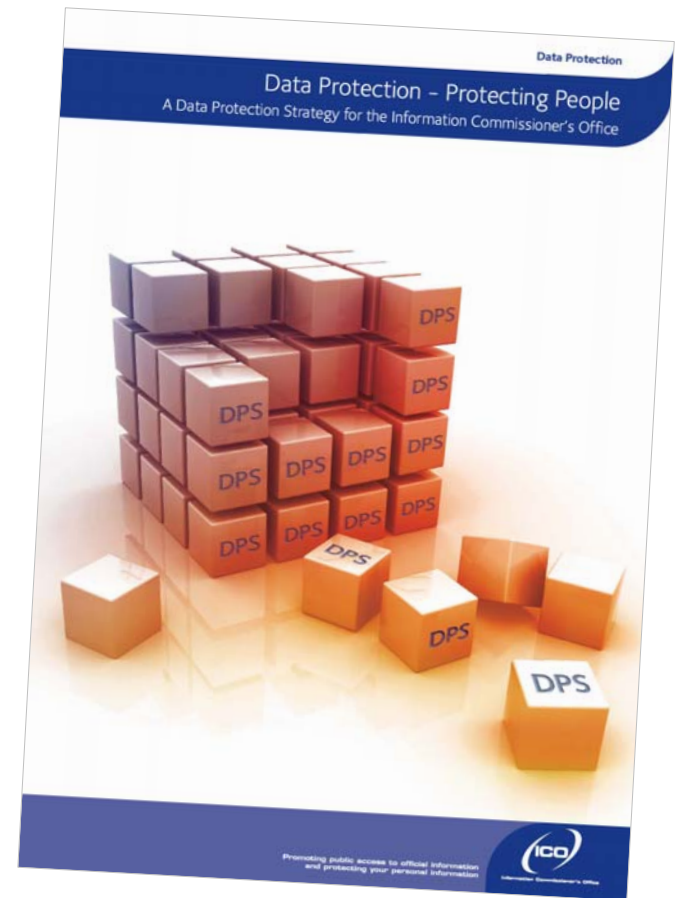
**Jonathan Bamford**

Assistant Information Commissioner  
Workshop F



# ICO Data Protection Strategy

- Building public confidence
- Minimising data protection *risk*
- Compliance with law not an end in itself – focus on *detriment* to individuals and society
- Being *selective to be effective*
- ‘Carrot and stick’ approach
- Maximising influence and impact



# ICO Data Protection Strategy: Key Areas for 2009-10

- Unlawful trade in confidential personal information
- Public security and surveillance
- Increased information sharing
- Privacy by design
- Security and integrity of information
- Effective data protection supervision

# Data Protection = 1<sup>st</sup> Social Issue

Research November 2008

- preventing crime 94%
- *protecting personal details* 94%
- National Health Service 88%
- equal rights 88%
- national security 87%
- improving education 87%
- environmental issues 87%
- protecting freedom of speech 85%
- unemployment 83%

# 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

# 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 launched 26 November 2008

# Privacy by Design Report

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

# Barriers

- A successful Privacy by Design approach will depend upon breaking down existing barriers
  - 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

# Delivering Privacy by Design

- Currently, unclear benefits and low risk of enforcement result in poor compliance, with little adoption of PETs or demand for products
- A 'Privacy by Design ecosystem' is envisaged

# Comparisons with Security by Design

- The report looked at how information security became a mainstream business issue
  - clearer understanding of the business threat
  - development of management standards (7799)
  - greater executive awareness
  - growth of language and professional networks
  - incorporation of CISO role into senior levels
- These are important achievements that can be echoed in the plans for Privacy by Design

# Engaging with executive management

- To ensure that 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

# Planning for Privacy by Design

- To ensure that 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

# Sharing Personal Information

- To assist the data sharing agenda whilst assuring individuals that their privacy will be respected
  - formalise approaches for collecting and managing privacy metadata
  - develop PIA approaches that can more easily take into account privacy implications of data sharing within and outside of organisations
  - define security controls for the protection of personal information in transit
  - promote data minimisation principles

# Developing Privacy Standards

- To provide organisations with consistent, affordable, provable privacy standards
  - government, industry and academia should be encouraged to collaborate on development of practical standards for privacy implementation
  - initiative needs to come from end user organisations so that outcomes are focused on their needs
  - engage with similar projects worldwide

# Promoting PETs

- To 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

# Compliance and Regulation

- To assure individuals that organisations will be held to account for proper processing of personal information, and to develop the privacy profession
  - greater accountability of executive management for respecting privacy rules
  - empowered ICO that can investigate and enforce that compliance
  - clarification of legal uncertainties to define meaning and use of personal information
  - creation of a professional body for privacy practitioners

# Future Action

- Supporting documents that provide greater detail about PETs and Security by Design are available at [www.privacybydesign.co.uk](http://www.privacybydesign.co.uk)
- Report recommendations have been reviewed by the ICO, and an implementation plan produced
- This is just the first step for Privacy by Design, and further research and delivery activities will follow

# Reputation and regulation matters for the Board

## Governance and Accountability

**Policies**

**Procedures**

**Contracts**

**Compliance**

**Technology –  
Systems**

**Architecture**

**Privacy by Design**

**People**

# The Personal Information Promise

- A chance to regain public trust and confidence by showing senior level commitment
- Not a regulatory compliance tool
- Opened for signature on European Data Protection Day (28 January 2009)
- PQs applauding those who have signed and questioning others who have not
- Media coverage

*I* (name and title),  
on behalf of (name of organisation)  
*Promise* promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing.

*Signed*  
Signed  
(name and title)

Date



# A look further into the year

- European DP Commissioners' Conference  
Edinburgh: 23 April 09
- Simplifying EU Directive research report: May
- Research project: economic argument for proactive privacy protection? Nov 09
- DP policy issue conference: Website related?  
Dec 09
- Another Commissioner's code of practice:  
Privacy and websites? Jan 10 consultation
- Report to Parliament on Surveillance
- Statutory information sharing code of practice?

# Privacy Incident Lessons Learned (PILL)

- On line account of privacy near misses
- Taps in to the wealth of experience of DPOs
- Not a substitute for security breach/regulatory notifications
- Aimed at DPOs who can profit from the experiences of others/share their experiences to benefit others

# PILL: Key Issues

- DPO involvement essential
- Won't identify organisations just nature of business
- Operated by 3<sup>rd</sup> Party to maintain confidentiality?
- Should it be just accessible by DPOs or wider?
- How to check authenticity?

# PILL: We need your help!

- Would it be helpful?
- Would you contribute?
- On what basis?
- Fill in our questionnaire and let us know!





**Information Commissioner's Office**

[www.ico.gov.uk](http://www.ico.gov.uk)