

Next generation data protection law

Iain Bourne
Information Commissioner's Office
(UK)

Corporate DP & Privacy
Compliance: Berlin 1-3-11

ico.

What does the ICO do?

Enforces and regulates:

- Data Protection Act
- Freedom of Information Act
- Environmental Information Regulations
- Privacy and Electronic Communications Regulations

Provides information to individuals and organisations

Adjudicates on complaints

Promotes good practice

Our performance

- c 212,000 – calls to our helpline
- c 2.06m – visits to our website

Data protection

- 33,234 – data protection cases received
- 32,714 – data protection cases closed
- c 328,164 – organisations notifying

Freedom of information

- 3,734 – freedom of information cases received
- 4,196 – freedom of information cases closed

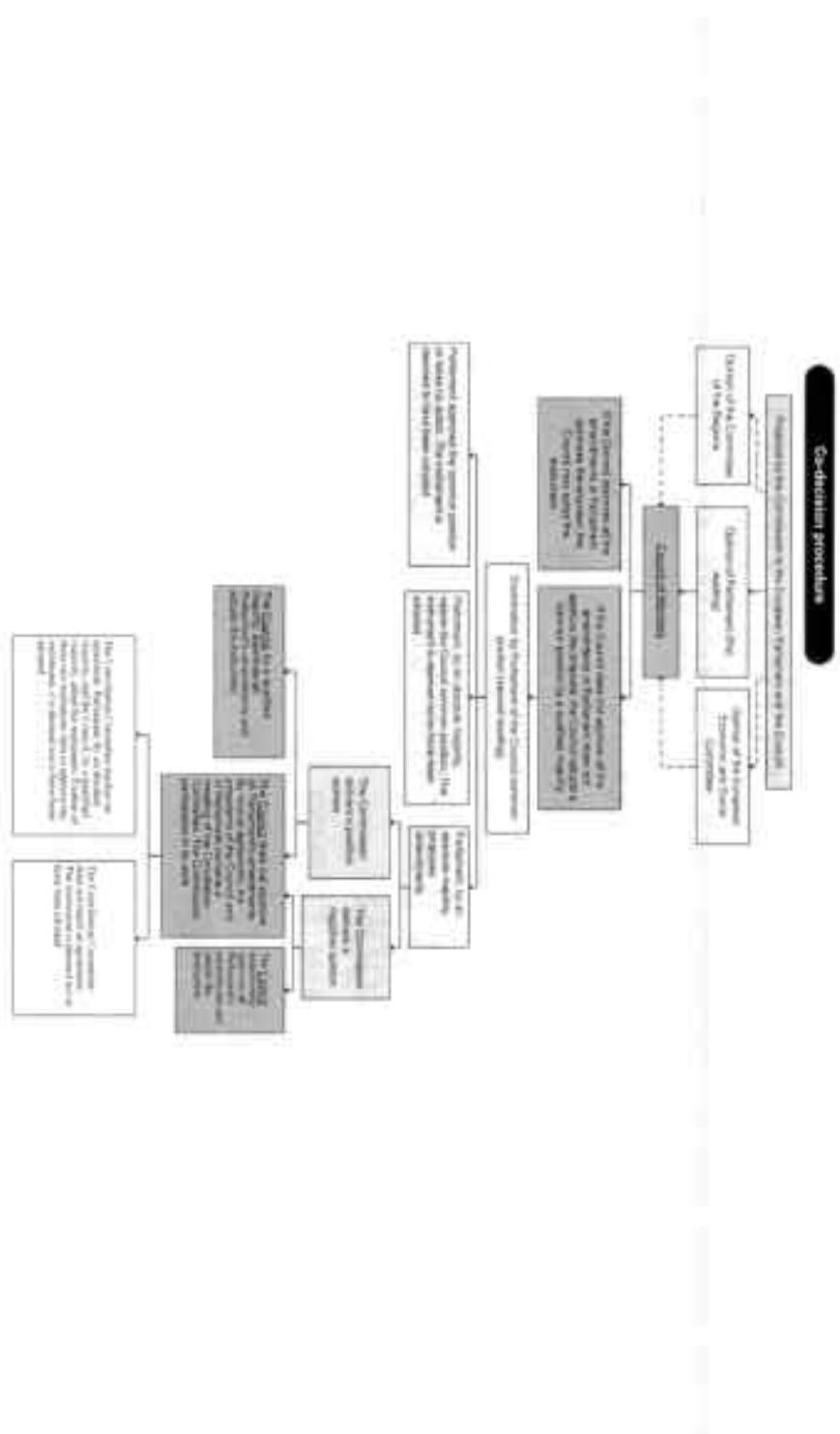
ico.

Current priorities for the UK's DPA

- Security breaches: lots of them
- Online and new technologies
- Implementing monetary penalties
- Developing audit function
- Surveillance society updates
- Revised E-privacy Directive
- Review of EU legislative framework
- Review of ICO guidance and policy development

A new data protection Directive

ico.



Review of EU legislative framework

- The current data protection principles are sound, but the law needs to achieve greater clarity of purpose and presentation. The principle of 'privacy by design' should be incorporated.
- Wide consensus over the value of the principles and of information rights
- What is the law there to do?
- Positive requirement for privacy enhancement – e.g. data minimisation

Review of EU legislative framework

- The law must provide greater clarity about what is personal data, with a more contextual approach to the sensitivity of information.
 - What sort of information should data protection law apply to?
 - Serious problems re: 'identified' / 'identifiable' - esp. online
 - Structure of information?
 - What is sensitive? Geo-location, finances, biometrics?

Review of EU legislative framework

- The law must be clearer about when consent is needed and what this involves.
 - High standard of consent in Directive
 - Danger of illusory or deceptive 'consent'
 - Consent as corporate indemnification
 - 'Informed' in complex information systems
 - Opt-ins, opt-outs, implicit consent, timing, revocation of consent...
 - Consent = freedom of choice

Review of DP legislative framework

- The approach the law takes to the responsibilities of data controllers and processors should better reflect modern business relationships.
 - Processors not passive entities
 - Degree of control over data processing
 - Stronger concept of collective responsibility
 - Shared liability - e.g. in enforcement cases

Review of EU legislative framework

- The law needs more realistic rules for international data flows.
 - Volume and speed of data flows
 - Difficulty (impossibility?) of meaningful regulation
 - Stronger responsibilities / liabilities of data exporters regardless of where the processing takes place
 - Risk-based guidance for potential exporters

Review of EU legislative framework

- The law needs to be more in tune with the Freedom of Information regime and to recognise the impact of modern technology on what private individuals do with personal information.

- Transparency Vs privacy tensions (technical and more fundamental)
- 'Citizen bloggers' and freedom of speech
- Responsibilities of online companies – e.g. social networking
- Role of Data Protection Authorities?
- Phenomena the Directive probably didn't anticipate

ICO recent projects

- 'Guide' to data protection
- Data sharing code of practice
- Personal information online code of practice
- Anonymisation workshop: legal difficulties and practical solutions
- Guidance for the public on Wi-Fi security
- UK govt. Rights and Freedoms Bill

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at [www.twitter.com/iconews](https://twitter.com/iconews)

ico.

Freedom of Information Disclosure

2-3 March 2011

Dawn Monaghan, Group Manager Public Services

AULP



The Right to Information - Givens

- The assumption of FOIA is the release of information held by 'public authorities' into the public domain
- Universities are defined as public authorities for the purposes of FOIA
 - All information held is covered by FOIA
 - Universities must comply with their obligations under FOIA
 - There is no 'blanket' exemption in the UK FOIA for research material
 - Information should be proactively made available, requests for information must be answered and information provided (unless exempt)

Background

- The ICO believes that generally universities cope well with information requests, however a few key high profile cases within the sector have;
 - a) Created a storm in the press with 'knock on effects'
 - b) Created 'fear' within the sector regarding requests
 - c) Caused concern about the ICO approach to research data
 - d) Generated 'The Muir Russell' Report

The Role of the ICO

- A regulator who implements and enforces the law, does not make it
- Ensures compliance of institutions the law defines as 'public authorities'
- Works with sectors to assist their understanding of the legislation
- Monitors the proactive release of information by authorities
- Investigates s50 complaints
- Requests and conducts voluntary audits of authorities who appear to be struggling with meeting the obligations of FOIA, including the Codes of Practice (s45,s46)

Proactive Release S19

- Adoption of the Model Scheme
- Using the HE definition documents produced by the ICO publish a 'guide to information'
- Expand and maintain that 'guide' on a regular basis with reference to new material and information provided through requests
- Possible expansion of routinely released datasets through 'right to data'

The ICO Approach to S19

- An integral and important part of FOIA
- Model scheme developed and approved by ICO for adoption by **all** public authorities
- Ongoing day to day routine release of information is the organisations responsibility
- Definition documents assist the process and provide sectoral consistency, they are guidance which can and will be regularly updated
- ICO Good Practice team Monitor 'adoption' and the requirement 'publish information in accordance'

Answering Requests for Information

- Respond within 20 working days
- If information is exempt, redact as appropriate
- Provide a refusal notice which clearly states what exemption/s have been applied and WHY
- If qualified exemptions, state a PIU has been applied and clearly explain the considerations for and against release
- Cannot withhold the complete document because some of the information is exempt
- When refusing information concentrate on the specifics of the case, don't base the refusal on general principles or assertions
- Explain the appeals process
- If requested conduct an Internal Review
- When communicating the outcome of review inform the applicant of the right to appeal to ICO

ICO Approach to S50 Complaints

- The onus is on the public authority to make the case for rejecting a request
 - ICO rule based on the case arguments put to them
 - The ICO will not make the case for the public authority
 - Each case is considered on its own merits
 - It is difficult to draw blanket inferences from previous cases
 - ICO concentrate on the specifics of the case and the arguments and reasoning put forward by the PA
 - ICO expect PA's to respond to them in a timely and considered manner
 - When being asked about the case it is beneficial for the PA to put forward their strongest and best arguments at the earliest possible stage.

Universities and Research Data

- The public has an interest in universities contributing to the UK's economic and reputational standing globally
- However, it is recognised open sharing of data at too early a stage could dissuade international collaborators from working with UK colleagues
- There are several exemptions which may apply to cases of research data

Research Data and the Exemptions

- S21 Accessible to the applicant by other means. Has the information already been published, is it being charged for by another organisation?
- S22 Intended for future publication. Does the information already have a future publication date associated with it and It is reasonable in all the circumstances that the information should be withheld until the publication date
- S 27 International Relations. Would release of the information prejudice relations or interests of UK abroad

Research Data and Exemptions

- S36 Prejudice to effective conduct of public affairs. Could the release of the information inhibit free and frank exchange of views in the future?

- S41 Information in confidence, but must be actionable breach of confidence

- S43 Commercial interests. Would disclosure prejudice the commercial interests of any person, including the public authority who holds it

Universities and FOIA

Competitive Markets and Commercial Interests

- The ICO recognise that universities as some other PA's operate in a global competitive context.
- ICO understands that universities themselves can have commercial as well as financial interests
- However, the existence of a commercial interest or competitive environment is not in itself enough to warrant the exemption from release of some information (such as teaching materials)
- Decisions must be taken on a case by case basis and there must be a demonstration of real potential commercial harm for the exemption to apply

Research Data -

Other Considerations

- Cost of compliance exceeds appropriate limit , in the case of universities £450
- Vexatious or repeated requests
- Be specific, be specific and be specific

Universities and Research Data

- Several exemptions are qualified and judgement calls must be made in these cases
- You must recognise that the outcome of certain cases may be strongly influenced by the public's right to know, this may be time sensitive
- There are tensions between DPA and FOIA, the onus is primarily on the PA to implement the requisite checks and controls to ensure that DPA is not breached
- The law assumes that a release of information under FOIA is a release into the public domain, therefore who is asking for the information is not pertinent to any decision to withhold

Lessons from Past Experience

- Universities can and do draw upon several exemptions when considering the release of research data
- When applying any exemption they must be clear and specific about why they are doing so and be able to defend their decisions
- There have been some high profile ICO decisions which have overturned the universities approach
- There have also been some ICO decisions which have upheld the decisions made by universities
 - FOIA must be compiled with
 - In this day and age the truth will out!

Future Developments

- ICO met with Universities UK, JISC and representatives from several universities in September to discuss research data. A sub group has been set up to discuss what issues should be explored and explained in ICO guidance
- The ICO hosts a HE sector panel every 6 months to discuss key issues and concerns within the sector
- Some representatives are keen to follow through on the 'research exemption' provided in the Scottish FOIA, the ICO may support this stance but will not be initiating it
- Definition Documents are to be revisited to better reflect the proactive release of research data

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at [www.twitter.com/iconews](https://twitter.com/iconews)

ico.

Regulating security: stronger sanctions, stiffer penalties

March 2011

RSA UK Security Management
Conference

Jonathan Bamford
Head of Strategic Liaison



The role of the ICO

- Enforce and regulate
 - Freedom of Information Act
 - Data Protection Act
 - Environmental Information Regulations
 - Privacy and Electronic Communications Regulations
- Provide information to individuals and organisations
- Adjudicate on complaints
- Promote good practice

The Data Protection Principles

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than necessary
- Processed in line with individuals' rights
- Kept secure
- Not transferred to countries without adequate protection

ico.

Seventh Principle: Security

- Must take appropriate measures taking account of:
 - nature of data and potential harm
 - state of technological development and cost
- Not just about technical security

Monetary penalties

- Introduced in April 2010
- Criminal Justice and Immigration Act 2008
- Penalty of up to £500,000 for serious breaches of DP Principles, committed knowingly/recklessly
- ICO statutory guidance

Amount of Penalty

- Nature of contravention
- Effect of contravention
- Behaviour of Data Controller
 - security breach notification?
- Impact on Data Controller
- Other Considerations

Assessment Notices

- Coroners and Justice Act 2009
- Power of audit in the absence of consent
- Government Departments – but could be extended to other public bodies and private sector
 - eg NHS Trusts
- Targeted consensual audit programme

ico.

Information governance

- Key lesson from data loss incidents
- Ownership and direction from the top
- Embeds privacy and DP concerns into the culture of an organisation
- Invest to reap 'The Privacy Dividend'
- Privacy impact assessments
- Privacy by design
- Can't be left to chance

Regulation is tightening

- Government's programme on openness, transparency, privacy and information rights
- E-Privacy Directive: mandatory breach notification
- Likely amendment to DP legislative framework in UK and EU

ico.

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at www.twitter.com/iconews

ico.
Information Commissioner's Office

Preparing guidelines and enforcing compliance

March 2011

PA 1

Dawn Monaghan, Group Manager Public Services



Preparing Guidelines

- Duty to promote Information Rights to the 'general' public
- May give advice to the general public
- Duty to promote 'the following of good practice by public authorities'
- Duty to promote observance by public authorities of the requirements of the legislation and the provisions of the codes of practice

Preparing Guidelines

Promoting to the public

- Leaflets and information on the website
- Answering mail and telephone enquiries
- Your rights
- How to ask for information
- What to do if you fail to receive the information
- How to complain to the ICO
- How to proceed to the Information Tribunal

ico.

Preparing Guidelines

Dealing with public authorities

- **First Contact Team** – Deal with mail and telephone enquiries simple and complex with reference to our 'Lines to Take' database and other experience
- **Policy Team** – develop the 'Lines to Take' (issued raised by public authorities, users of the Act or Decision Notices) write guidance for public authorities and publish it on the website
- **Strategic Liaison** – Build and maintain relationships with key sectoral stakeholders, give advice and guidance at the early stages of new structures, initiatives, projects etc which have potential impacts on Information Rights

Preparing Guidelines

Criteria

- Clear and concise
- Targeted
- Timely
- Correct language
- Correct format
- Correct outlets primarily website but not solely

Preparing Guidelines

The Journey

- Short Term – Thinking out loud
- Medium Term – Developed thinking
- Long Term – Case law and experience driven

Preparing Guidelines

What do authorities want to know?

- What is the minimum we need to put in place?
- Which exemption can we use as a catch all?
- When and how will we apply the public interest test?
- What are the benefits?
- How do I get 'buy in' at the top

ico.

Preparing Guidelines

What do the general public want to know?

- What information can I have access to?
- When can I access it?
- How can I access it?
- What will it cost?
- What do I do if I'm unhappy with the response?

Preparing Guidelines

What is it really all about?

- Openness and trust
- Communication external and internal
- Changing culture and working practice
- Information handling, records management
- Customer service
- Accountability

ico.

Preparing Guidelines

Main areas

- Proactive dissemination
- Exemptions
- Public Interest Test
- Commissioners policies and procedures
- Technical – Are we a PA, which legislation?

Enforcing Compliance

- Complainants can apply to the Commissioner
- The Commissioner has powers to issue notices:

 - Information Notices
 - Decision Notices
 - Enforcement Notices

- Notices can be appealed to the Information Tribunal

ico.

Enforcing Compliance

Information Notice

- Compel a public authority to provide information to the commissioner for his consideration
- Can be appealed to the tribunal

ico.

Enforcing Compliance

Decision Notice

- Issued to public authority and to the complainant
- States whether the Commissioner agrees or disagrees with the PA and why, and details any actions required
- Either party can appeal to the Tribunal

ico.

Enforcing Compliance

Enforcement Notice

- Served on a public authority for non compliance:
 - Failure to comply with the requirements of Part I;
 - or
 - Non adoption of a scheme
 - Can be appealed to the Information Tribunal

ico.

Enforcing Compliance

Practice Recommendation

- Served on a public authority if persistent or serious breach of the Codes of Practice
- Not enforceable, not a notice
- Public authority can ignore
- Breaches of Codes may also be failure to comply with Part 1 and lead to enforcement

ico.

Enforcing Compliance

Non compliance with a Notice

- Commissioner can write to the High Court
- Information Notices – Failure to comply includes making a false statement
 - The Court may inquire into the matter
 - May find the public authority in contempt of court
 - Penalty, a fine or up to 6 months imprisonment

Enforcement Strategy

- Use of enforcement notices for serious and significant breaches

- Undertakings for FOIA and EIR as well as DPA

- Approach to monitoring and use of trigger points

ico.

Enforcement Strategy

Section 10

- 20 working days to respond to a request
- When applying the PIT can be extended to 40 working days
- Approx 1/4 of casework concerned with failure to meet the time for compliance

Enforcement Strategy

Triggers

- 6 or more failures to meet timescale in a 6 month period
- For Gov Dept's. Less than 85% compliance as shown in MOJ stats
- Delay of more than 15 days over limit (35 or 55 days)

ico.

Enforcement Strategy

Triggers

- If hit 'triggers' appropriate for assessment
- Discussion with authority regarding reasons for delays
- 'Common sense' filter with regard to whether assessment undertaken

Enforcement Strategy

What happens next!

- Monitoring for up to 3 months
- Interacting with PA to make informed decisions about appropriate ways forward
- Each month stats submitted to ICO
- If improvements seen monitoring ceased and no further action taken
- Failure to improve could result in an enforcement notice (s10/reg5)
- Could also result in a practice rec. or an undertaking if other issues discovered

ico.

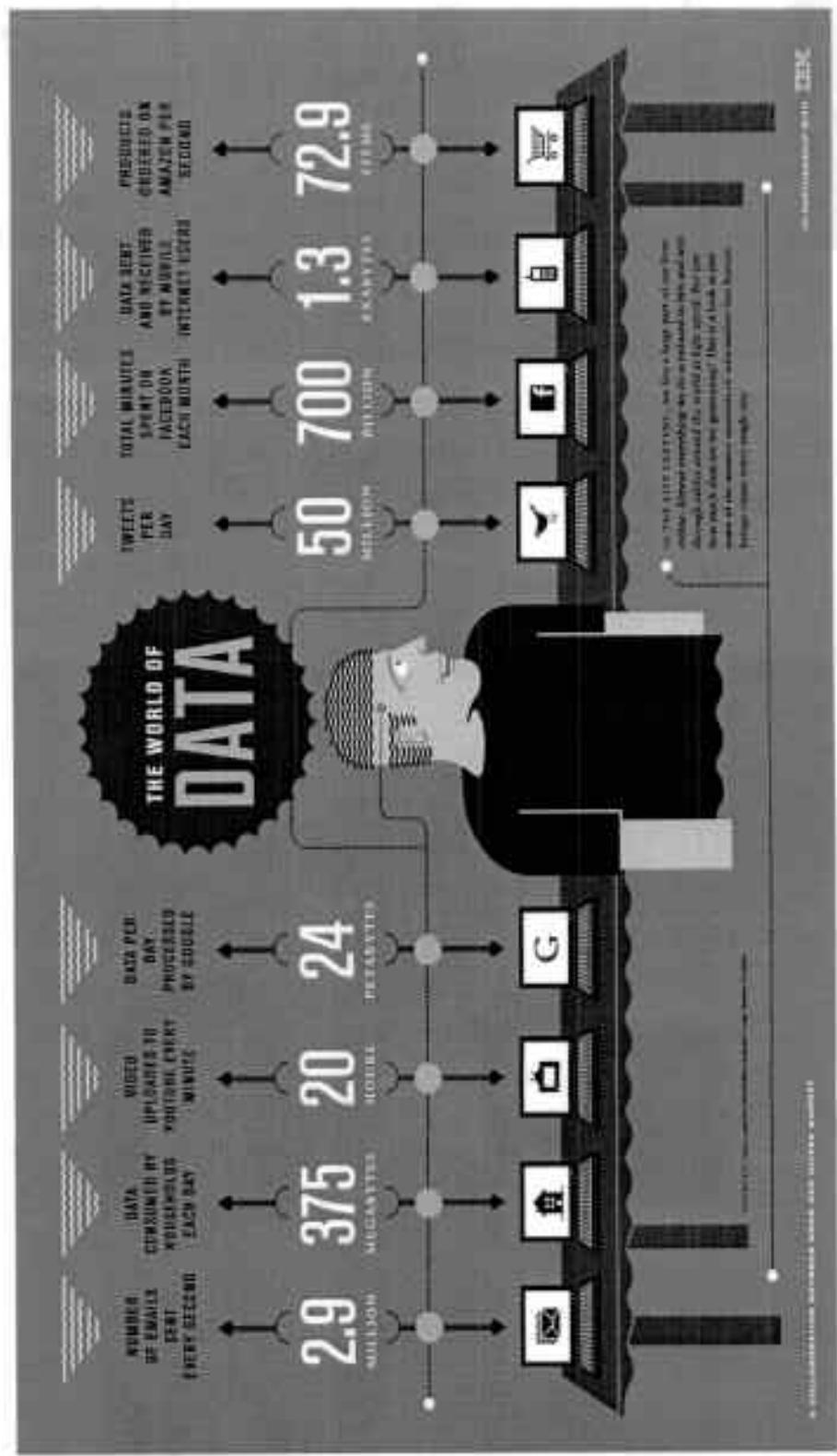
The case for Privacy by Design

SCL Privacy & Data Protection Group
Meeting, 16 March 2011

Steve Wood, Head of Policy Delivery, Information
Commissioner's Office



Context



ico.
Information Communication Company

Public concern

- Individuals continue to show concern about the issue of protecting personal information

Q1 I am going to read out a list of issues that could be considered of social importance. Please tell me how concerned you are about each of the following issues.²

Prompted	2004	2005	2006	2007	2008	2009	2010
Preventing crime	85%	88%	93%	94%	94%	96%	93%
Protecting people's personal information	70%	83%	83%	92%	94%	94%	92%
Unemployment	50%	70%	72%	80%	83%	93%	90%
The National Health Service	78%	83%	90%	91%	88%	90%	90%

*ICO Annual Track research 2010: individuals

ico.

Privacy by Design

- Privacy is not dead but approaches to compliance must keep pace with technological change and emerging risks
- An approach to reduce the risks arising from processing personal information and rebuild consumer trust
- Privacy by Design Lifecycle approach
 - due consideration to privacy needs prior to the development of any new system or process
 - maintain that control throughout the systems lifecycle
- Use of Privacy Impact Assessments (PIAs), Privacy Enhancing Technologies (PETS)

Privacy by Design: business case

- The privacy value of personal information
- The consequences of privacy failures
- The benefits of protecting privacy
- The investment needed for the protection of privacy
- Organisations and the market need a 'nudge' or firmer push?

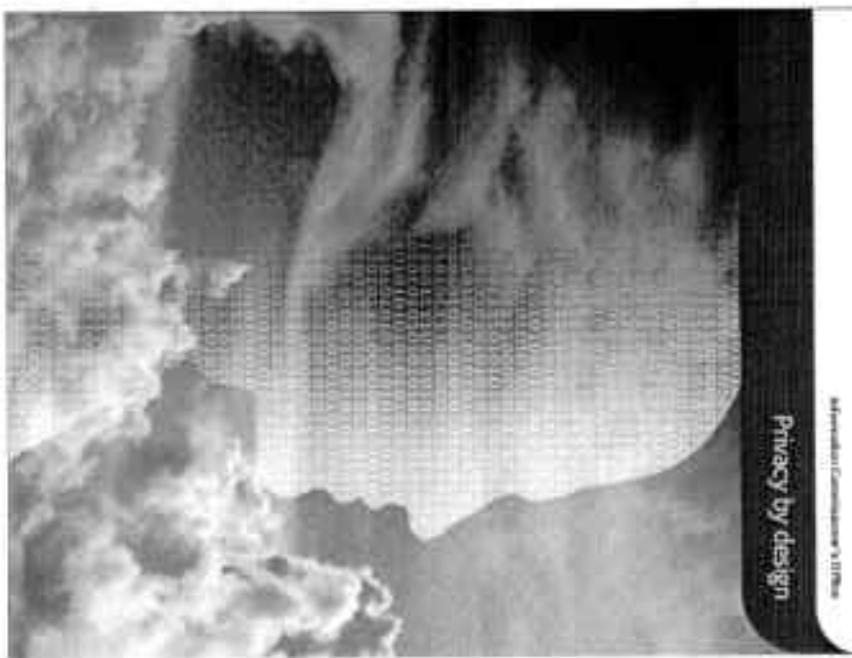
Privacy by Design: legal drivers

- Article 17 of Directive 95/46/EC - requires appropriate technical and organizational measures to protect personal data against unlawful forms of processing
- Recent EC proposal: A comprehensive approach on personal data protection in the European Union COM(2010) 609 final:

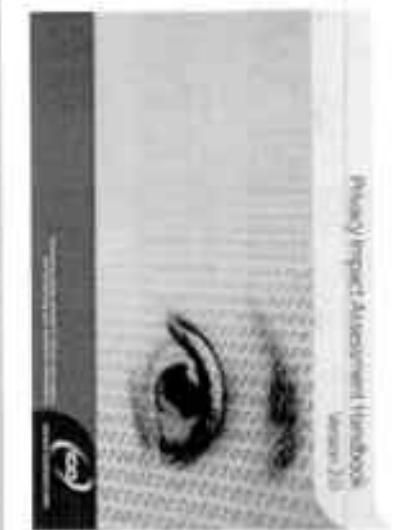
"including in the legal framework an obligation for data controllers to carry out a data protection impact assessment

further promoting the use of PETs and the possibilities for the concrete implementation of the concept of 'Privacy by Design'."

Privacy by Design: tools and guidance



The Privacy Dividend:
the business case for
investing in proactive
privacy protection



ico.

ico.

http://www.ico.gov.uk/news/current_topics/privacy_by_design.aspx

Examples of where Privacy by Design can make a difference

- Legislative and design stages of large IT projects, particularly in the public sector
e.g. Smart Metering
- Identity Management Systems, included federated ID mgt
- Emerging challenges
 - Mass market uses of facial recognition technology
 - Location based technologies
- European Privacy Seals
<https://www.european-privacy-seal.eu/awarded-seals/de-110022>

Privacy by Design: challenges

- PETS – making the right investment choices
- Challenge of identification, pseudonymisation and anonymisation
- More examples, case studies and evidence of benefits needed
- Getting individuals to understand the risks and benefits of putting more of their information in the public domain

ico.

Privacy by Design: future work by the ICO

- Review and update P by D guidance
- Further research into case studies
- Further work on the risks of anonymisation and new guidance.
- Expanding technology expertise: New Technology Adviser:
Simon Rice

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at www.twitter.com/iconews

ico.

387 - Sliding

- Col

- with ICO Rec
+ 200k

①

When things go wrong: information governance breaches and the role of the ICO

16/3/2011

David Evans, Senior Policy Officer



16th MARCH 2011

Trust of providers

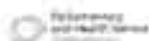
- will have less

Information Services - Service etc
around

will need not a Service

trust you receive directed
or qualified Trust

A salutary tale



A Breach of Confidence

A report by the Parliamentary and Health Select Committee on an investigation
of a complaint about HM Revenue & Customs, the Child Support Agency and the Department for Work and Pensions.

ico,

white paper
confidence issue
clarification

I recommend it!

- Not about a major story
in the media
or Government's blunder
100s or 1000s of pages

RAT 100



In brief

- HM Revenues and Customs
- Child Support Agency
- Department for Work and Pensions

ico,

house (house) 1.000000

Major mistake

Then there's bodies

6

What happened

- Complainant (Ms H) dealing with a number of govt agencies had address incorrectly changed
 - Error duplicated
 - When error pointed out it was not corrected
 - No one took responsibility

fco.

Consequences for Ms M

- Ms M's personal data sent to former partner
 - Unexpected decrease in child support
 - Time and effort spent trying to establish what had gone on
 - Stress

ico.

Outcome

- Complaint to Parliamentary Ombudsman
 - Detailed investigation
 - Adverse outcome - maladministration
 - Cost - actual and reputational

100.

- Spez. feste Partie

Software in CS Adminstration
we know "UPDATES" in Linux +

Gave Mrs. M. some address

As the writer thinks

- Edge Trunk Reduction

Time Other Dots

4

Results. © As Seen On TV with its

Sonic birth gender break

Customer Color Service Options

A More Detailed Work Plan

So little Everyone will take to fit

To The Editor - A Message of Truth

Mr. Murphy

Outcome

- Complaint to Parliamentary Ombudsman
- Detailed investigation
- Adverse outcome - maladministration
- Cost – actual and reputational

ico.

- Police Investigation

- Organisational Time & Effort
 - Up to V. Service / Police

- organisational cost.

+ It was my responsibility

(many were given at same time)

submissions ^{more} ~~more~~ received from the public

→ No One Took Responsibility

- Meeting arranged

- Concerned the Police

- + All + the more time // were

MEET
LET ME READ THIS

(4)



LONDON, 17/11/07

More outcomes

In her response to a draft of this report, Ms M said that trying to sort this problem out had made her very distressed and had impacted on her family life. She felt she could not move on from her separation from Mr A as the address itself provided a constant reminder of a very unfortunate episode in her life. Ms M said she was particularly concerned because she took a lot of trouble trying to separate her and Mr A's affairs when they split up so that her credit rating was not adversely affected by his debts. She is still concerned that there may be some link between her and Mr A's affairs within a government department, which may cause her problems again in the future.

Having read the draft report, Ms M commented that she was shocked, to say the least, that agencies she had trusted appeared to have lied to her Member of Parliament, made errors, and delayed the investigation until such time as an audit trail was no longer available. Ms M said that this left her in a situation where she would never know why the error had happened, she would never have peace of mind that it would not happen again and she would never trust a government agency again. Ms M said that she found all of this quite disturbing and 'bad'

ico.

*£2,000 damages awarded to Ms M
as small award - But Glaxo Smith
Kline required to review its IT systems*

More outcomes

In its response to a draft of the code of practice, and following its own consultation, the ICO has decided not to proceed with the code. Instead, it has decided to issue a statement of principles, which will set out the key principles that should underpin data sharing between organisations. The ICO believes that the statement of principles will help to support best practices in data sharing, and that they will go some way towards addressing the concerns raised by the public and other stakeholders. The statement of principles will be published in due course.

ICO

Setting out the draft code of practice, the ICO has decided to issue a statement of principles, which will set out the key principles that should underpin data sharing between organisations. The ICO believes that the statement of principles will help to support best practices in data sharing, and that they will go some way towards addressing the concerns raised by the public and other stakeholders. The statement of principles will be published in due course.

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

With this? This goes back to what's at the start.
+ NOT much added to what's at the start.

Data Sharing Code of Practice

The code covers the two main types of data sharing:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

ICO

- Lawton done 11 May 4.1C

This is MARK - coming
from my friend

Data Sharing Code of Practice

Who should use this code of practice?

Any data controller who is involved in the sharing of personal data.

How the code can help:

 Adopting the good practice recommendations in the code will help you to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

ICO

⑥ Remember to write
for these individuals who
are key!

6

Status

- Statutory code.
- Approved by the Secretary of State and laid before Parliament
- The code does not impose additional legal obligations nor is it an authoritative statement of the law.
- The code can be used in evidence in any legal proceedings, not just proceedings under the DPA.

ico.

Benefits

- inspiring public trust by helping ensure that legally required safeguards are in place and complied with;
- better protection for individuals when their data is shared;
- greater trust and a better relationship with the people whose information you want to share;
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data.

ico.

More benefits

- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or consent in the face of objection;
- minimised risk of breaches and consequent enforcement action by the ICO or other regulators; and
- reduced risk of questions, complaints and disputes about the way you share personal data.

ico.

① Safeguard - Change from
seminar to Data Sharing Code

→ AGMs →

② Clarifying the necessary law
from relevant + cover
the Data Protection

③ Introducing basic terms
→ key to sharing better covers

④ Reputations & Risk

- costs £79 per £300 monthly

→ Greater REPUTATION

£700 p/a
£30,000 p/a + 10%

- All Good Stuff

* Now if it goes wrong

7

log

If things go badly wrong

recovery domain
process

- ① • Containment and recovery
- ② • Assessment of ongoing risk
- ③ • Notification of breach
- ④ • Evaluation and response

ICO.

① Damage limitation

- communicate HR, IT, Legal & Risk
evaluate what needs to
be done to fix the issue

- who do you need to tell? - tell certain the board
- network or even senior execs

② - what type of data is involved?

- how sensitive is it?
- is it encrypted?
- has it been stolen?
- how many people are affected?
- what's the potential harm

③ notification steps (how it came from)

- by law factors like privacy, telecommunications
also businesses can do

↓ over →



3

If things go badly wrong

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

ICO.

Reporting to the ICO

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Action taken to minimise / mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information you feel may assist us in making an assessment

ICO.

If you Do Report The Breach
To The ICO
This Is What We'll
Do

LOWEST

What the ICO can do

- Investigate and assess
- Enforcement
- Monetary Penalty Notice

ICO.

① Action or Not - Depending
on Circumstances

② Not Punishment - Low
Level Conduct Continues

③ Administrative Punishment

(a)

Monetary Penalties

- ICO can serve a Monetary Penalty Notice on a data controller
- Require payment of a Monetary Penalty which must not exceed £500,000
- Applies to all data controllers in the private, public and voluntary sectors

ICO.

① Why is there more because
it's the Justice Sector
- if it's serious we
will ACT

Monetary Penalties

- Before the ICO can impose a Monetary Penalty it has to be satisfied under section 55A that:
 - There has been a serious contravention of the data protection principles by the data controller
 - The contravention was of a kind likely to cause substantial damage or substantial distress and either:
 - The contravention was deliberate or,

ICO.

Serious
- May be deliberate (intend)
or不慎的 (careless)

Monetary Penalties

- The data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention

ICO.

Gross Negligence
- may be carelessness
or carelessness of
overlooked
what were serious were
unconscio

Contravention was deliberate

- The contravention was deliberate or premeditated
- Data Controller was aware of and did not follow relevant advice published by the ICO and others
- Series of similar contraventions and no action taken by data controller to rectify cause of original contravention

ICO,

→ Action Theory Works - In
Practice But Not
Reflected in Practice



Failed to take reasonable steps to prevent the contravention

- Inadequate procedures, policies, processes and practices in place
- No clear lines of accountability
- Failure to implement guidance or codes of practice published by ICO or others

ICO,

X Heats - FAX (from Frank Cannon)
- Twice
- Cried Name / ~~Not~~
- Once ~~Not~~

What happens? - Notice of Intent

- ICO must serve a data controller with a Notice of intent setting out the proposed amount
- The Notice must also contain prescribed information and provide the data controller with at least 21 days to provide written representations to the ICO

ICO,

(1)

MPN Summary

- Applies to ALL Data Controllers
- Only applies to **serious contraventions** of the data protection principles
- Notice of Intent
- Monetary Penalty Notice
- Appeal to the Tribunal

ico.



ico.

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at www.twitter.com/iconews

ico.

Recovering losses & Warrantability

- Minor - Unwarrantable

Ending of Unlawful Practices

- MPN

- Both - Policy breached

- Practice - NOT Encrypted

→ too sensitive info
being used to store
complaints sensitive P.O.

Stay Safe

① Tell individuals to keep

② Update software /

ICO Policies

④ Use the massive Oct

Tools To Help You

