Why are we doing all this?

The imperative of data protection compliance

Christopher Graham
UK Information Commissioner

24th Feb 2011

Our Mission

The ICO's mission is
to uphold information rights
in the public interest,
promoting openness by public bodies
and data privacy for individuals.

ico.

The role of the ICO

- Enforce and regulate
  - Freedom of Information Act – but not FOI(S) Act
  - Data Protection Act
  - Environmental Information Regulations
  - Privacy and Electronic Communications Regulations
- Provide information to individuals and organisations
- Adjudicate on complaints
- Promote good practice

ico.

Revising the Directive

- Rand Europe review
- Using our influence
- Article 29 Working Party
- Working with MoJ
- Implementation

ico.

The digital deluge

- Lean times
- Coalition commitments
- Monetary penalties
- Technological developments
- Access and accountability

ico.

Who's in the driving seat?

1980s

A few online service providers
Internet virgin consumers

2011

Universal online service provision
Consumers who are savvy and empowered

ico.

Public social concerns

Q1: I am going to read out a list of issues that could be considered of social importance. Table shows respondents who were either 'very concerned' or 'fairly concerned' about each issue.

Social Issue	Overall		
	2004	2009	2010
Preventing crime	85%	96%	93%
Protecting people's personal information	**70%**	**94%**	**92%**
Unemployment	50%	93%	90%
The National Health Service	78%	90%	90%
Improving standards in education	76%	89%	90%
Equal rights for everyone	69%	89%	87%
Protecting freedom of speech	67%	89%	86%
National security	71%	90%	85%
Environmental issues	66%	90%	83%
Access to information held by public authorities	**48%**	**80%**	**75%**

ico.

Source: ICO Annual Track 2010/11

- For all issues there are lower levels of concern than 2009
- Less concern about access to public information
- Very high levels of concern regards protecting personal information

People care about their data

Bad practice
- Alienates customers
- Disillusions citizens

Good practice
- Retains customers
- Engages citizens

ico.

Monetary Penalties

- Since April
- Up to £500,000 'fine' for Data Controllers
- Serious breach of the DP principles
- Substantial damage or substantial distress
- Deliberate or reckless:
  - knew or ought to have known
  - failed to take reasonable steps to prevent
- Four CMPs to date
  - Herts County Council
  - A4e
  - Ealing and Hounslow LB

ico.

Audits

- Educate and assist organisations to meet their obligations
- Deliver practical and pragmatic advice and recommendations for organisations
- Use a risk based approach to focus activity in the areas where the ICO can make the best use of its resources
- Assist the ICO to share knowledge and promote good data protection practice through publishing audit outcomes
- Allow organisations to show their commitment to, and recognition of, the importance of data protection

ico.

Here to help

- Better Regulation approach
- Advice
  - Personal Information Toolkit
- Guidance
  - Data Sharing Code – May 2011
- Website www.ico.gov.uk
- ICO Scotland

ico.

ePrivacy Directive

- Due in May
  - 'Cookie consent'
  - Compulsory breach notification by Tel Cos
- Working with BIS
- Industry must prepare – not bury heads
  - Information to consumers
  - Privacy friendly default settings
  - User control
- Substantial work needed
  - Regulations
  - Guidance
- Better to implement later following adequate preparation

ico.

Sec 55 breaches

- Human factor the weakest link
- Blagging personal information
- Selling personal information
- Victimless crime?
  - Debate recovery
  - Divorce settlements
  - Custody battles
  - Witnesses, juries
  - 'suckers lists' for prize mail scams
- We need a more effective deterrent
- Threat of going to prison

ico.

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

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

ico.

Civil Monetary Penalties

Ken Macdonald
Assistant Commissioner

Holyrood Data Protection Conference
24 February 2011

Information Commissioner's Office

Content

ico.
Information Commissioner's Office

Options for Regulatory Action

Options for Regulatory Action

Pre-2011

Undertakings

Enforcement Notices

Prosecution

ico.

Options for Regulatory Action

Criminal Justice & Immigration Act 2008
s144 Power to require data controllers to pay monetary penalty

SI 2010/31 The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010

SI 2010/910 The Data Protection (Monetary Penalties) Order 2010

ico.

Assessing the Penalty: I

Monetary Penalties - ICO Guidelines

Monetary Penalties - ICO Guidelines

There has been a serious contravention of section 4(4) of the Data Protection Act 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,

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.

Monetary Penalties - ICO Guidelines

Seriousness of contravention

The contravention is or was particularly serious because of the nature of the personal data concerned;

The duration and extent of the contravention;

The number of individuals actually or potentially affected by the contravention;

The fact that it related to an issue of public importance, for example, unauthorised access to NHS Emergency Care Summaries

The contravention was due to either deliberate or negligent behaviour on the part of the data controller

ico.

Monetary Penalties - ICO Guidelines

Likelihood of substantial damage or substantial distress

The contravention was of a kind more likely than not to cause substantial damage or substantial distress to one or more individual.

ico.

Monetary Penalties - ICO Guidelines

Deliberate contravention

The contravention by the data controller was deliberate or premeditated;

The data controller was aware of and did not follow specific advice published by the Commissioner or others and relevant to the contravention; or

The contravention followed a series of similar contraventions by the data controller.

ico.

Monetary Penalties - ICO Guidelines

Reckless contravention

The likelihood of the contravention should have been apparent to a reasonably diligent data controller;

The data controller had adopted a cavalier approach to compliance and failed to take reasonable steps to prevent the contravention, for example, not putting basic security provisions in place;

The data controller had failed to carry out any sort of risk assessment and there is no evidence, whether verbally or in writing, that the data controller had recognised the risks of handling personal data and taken reasonable steps to address them;

ico.

Monetary Penalties - ICO Guidelines

Reckless contravention (con't)

The data controller did not have good corporate governance and/or audit arrangements in place to establish clear lines of responsibility for preventing contraventions of this type;

The data controller had no specific procedures or processes in place which may have prevented the contravention (eg, a robust compliance regime or other monitoring mechanisms)

Guidance or codes of practice published by the ICO or others and relevant to the contravention were available to the data controller and ignored or not given appropriate weight.

ICO.

Assessing the Penalty: II

Monetary Penalties - ICO Guidelines

Most serious situations only

Sector, size and resources of the DC

Not intention to impose serious financial hardship

ico.

Monetary Penalties - Examples

Hertfordshire County Council - £100k

Highly sensitive personal information faxed to the wrong recipients – twice.....

A4e - £60k

Loss of unencrypted laptop containing details of 24,000 people who had sought legal services

ico.

Keeping in Contact

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

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

Contact us on 0131 301 5071 or at
scotland@ico.gsi.gov.uk

ico.

Holyrood Data Protection Conference

24 February 2010

Workshop 1 – The New Powers and Penalties of the ICO

Ken Macdonald, Assistant Commissioner (Scotland & NI)

Case Study 1

As part of its recruitment procedures, a company sought information about applicants from a consultant who maintained a database of persons who had previously worked for other organisations in the same sector. The database contained details of individuals' sensitive personal data relating to their trade union activity, their previous employment conduct and other information of a political nature.

Having been altered to this practice, and after investigation, the Commissioner found that the data controller had contravened the First Data Protection Principle. It had processed personal data unfairly by obtaining personal data and failing to provide the affected individuals with the appropriate fair processing information. In addition, the Commissioner considers that none of the conditions in Schedules 2 and 3 to the Act have been met, despite the processing of sensitive personal information being undertaken.

The Commissioner issued an enforcement notice against the organisation requiring it to comply with the First Data Protection Principle, his most powerful enforcement action at that time. In your view, would that breach have warranted a civil monetary penalty had it been in the Commissioner's powers to levy one and, if so, what level of penalty would have been appropriate ?

Case Study 2

A major retail store contracted out the processing of certain aspects to its pension scheme to another company, requiring the personal details of relevant employees to be passed to the data processor. The total number of employees on the database was 26,000.

The Managing Director of the data processing company then downloaded the database on to his unencrypted laptop to assist him in the preparation for a meeting he was to have with the client. Two days later, his laptop was stolen following an incident at his house.

The Commissioner issued an enforcement notice against the organisation requiring it to comply with the Seventh Data Protection Principle, his most powerful enforcement action at that time. In your view, would that breach have warranted a civil monetary penalty had it been in the Commissioner's powers to levy one and, if so, what level of penalty would have been appropriate ?

Practical application: some examples and the ICO view

Dave Evans, Group Manager – Business and Industry Group
Information Commissioner's Office

16th Feb 2011

The ICO's role

- Our statutory duties are to enforce the law, deal with complaints and provide good practice advice.
- Part of that last point has to involve letting people know what our priorities are.
- We focus on the risk of privacy detriment as well as the risk of damage or distress.
- We will seek to ensure compliance through enforcement as a last resort.

ico.

Scenario one

- What are the key factors to identify? What do you need to know before you can advise?
- What are the relevant legal provisions?
- What about good practice – going beyond what the law requires?
- What are the risks?

ico.

Scenario two

- What are the regulatory requirements here?
  - DPA98
  - PECR
- How might the Trust comply?
  - Would a 'no marketing' option suffice?
  - How might they get consent?

Scenario three

- This occurs most often with commercial companies rather than charities
- Would charities and fundraisers consider this sort of approach?
- If so what are the risks?
- Can this sort of 'lead generation' comply with the legislation?
- If so, how?

ico.

Scenario four

- Has the law been breached here?
- What rights does the supporter have?
- What other regulatory consequences might arise from this scenario?

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

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

ico.

Scenario One

FightCancerCheshire want to contact their own existing supporters with information about a new campaign they are launching with another charity, BattleCancer NorthWest. BCNW are struggling in the current economic climate and think their supporters would appreciate being included in the new campaign.

FCE have not contacted their own customers for some time but are confident that they would expect to receive marketing. However they are more concerned about contacting people whose details were originally collected by BCNW.

FCE are aware that BCNW have a good reputation and have received assurances that the information was collected in line with the requirements of the Data Protection Act (they have been told that supporters are aware their details may be passed to third parties) but they are not sure if it was collected on an 'opt in' or 'opt out' basis.

Scenario Two

The Woodside Trust is a conservation charity. They are running a competition in a national newspaper as part of their campaign encouraging people to make more use of Britain's woodlands. Entry to the competition (to win a holiday in one of their woodland cabins) is by texting the word 'HOLIDAY' to a short code.

The Trust wants to telephone the unsuccessful entrants. During the calls they will let people know that their entry was not successful. They then want to go on to provide people with some more information about the work the trust is doing in their area, and to encourage them to come along to local events.

They want to know what they would need to put in the advert to allow them to telephone these people. They do not want to screen the numbers against the TPS as they are a charity and cannot afford to pay thousands of pounds for the list.

Scenario Three

Homefone are running a 'Friends and family' promotion which means individuals can nominate 5 friends and family to get free calls to *if* they sign up with that company. The company has three options and wants to know the implications of the PECR on each one.

- To email their own customers (they have consent to send marketing emails to their own customers) and get their customers to forward the email on to their friends and relatives, the email will contain a link to the Homefone website which explains more about the offer and tells them how to sign up.

- To send their own customers a form which asks them to complete the email addresses of the 5 people they wish to recommend. The company will then email these recommended individuals directly with a link to the Homefone website and information about the offer.

- To do either of the above but also offer their customers a £10 discount on their bill for each recommendation they make.

Scenario four

Mr Jones is in high dudgeon. An error by your online team led to supporter details being published on your website. As a supporter, Mr Jones is annoyed to find that his details have been made available to the world.

He contacts you to inform you that since the incident he has noticed suspicious transactions on the account he uses to send you donations each month. He is also investigating whether his credit file contains fraudulent applications for credit.

The Changing Face of Data Protection Legislation and Compliance

David Smith
Deputy Commissioner

2nd Feb 2011

ico.
Information Commissioner's Office

The legal framework

- Data Protection Act 1998
- EU Directive 95/46/EC
- Privacy and Electronic Communications Regs 2003 (PECR)
- EU Directive 2002/58/EC
- EU Directive 2009/136/EC

ico.

PECR changes

- Consent for cookies
- Specific security requirements
- Breach notification
- Supervisory powers

ico.

DP Directive Review

- Commission communication
- Breach notification
- Accountability
- Data minimisation/Privacy by Design
- Right to be forgotten
- More effective supervision

ico.

ICO powers

- Criminal prosecution
- Enforcement Notices
- Assessment Notices
- Monetary Penalties

ico.

Monetary penalties

- Introduced April 2010
- Up to £500,000
- Serious breaches committed knowingly/negligently
- ICO statutory guidance
- Depends on nature/effect of contravention
- First penalties imposed

ico.

Assessment notices

- Introduced April 2010
- Power of audit in the absence of consent
- Government departments – but could be extended
- Code of Practice published
- ICO aims for co-operation

ico.

ICO experience

- Data breaches continuing
- Theft/loss of portable media significant
- Retention/lack of weeding a problem
- Communications/training/awareness a frequent factor
- Policies/procedures not related to jobs
- Need to monitor contractors/processors
- Room for improvement in governance

ico.

ICO approach

- No 'toothless bulldog', but primary focus is education, awareness, good practice
- Strengthening public confidence by making it
  - easier for the majority of organisations who seek to handle personal information well
  - tougher for the minority who do not

ico.

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

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

ico.