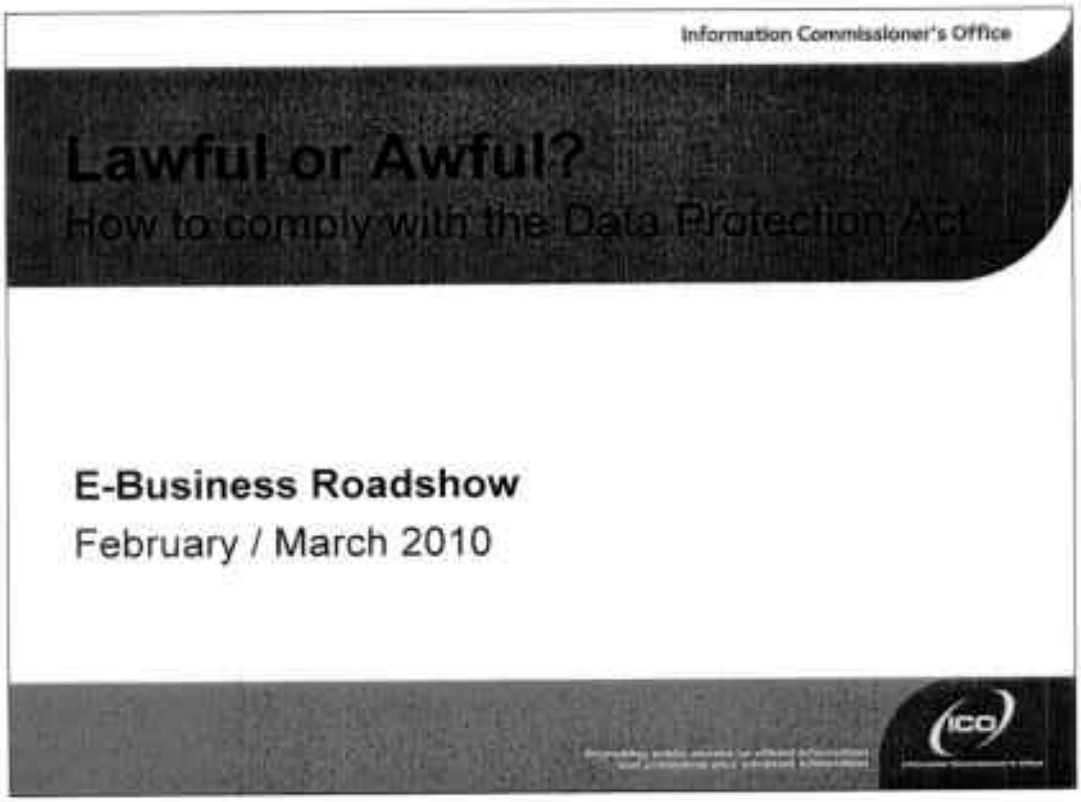
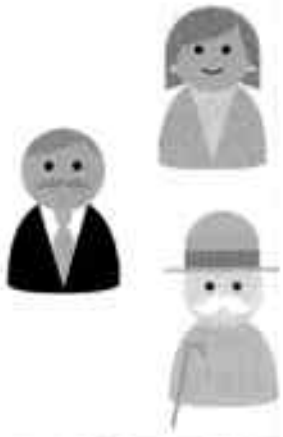

Information Commissioner's Office
Lawful or Awful?
How to comply with the Data Protection Act
E-Business Roadshow
February / March 2010

ICO's role

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

Why is compliance important?

- ☹ Get it wrong and there are consequences!
- ☹ Harm to individuals
  - Loss of control and privacy
  - Physical harm
  - Financial harm
- ☹ Harm to your business
  - Loss of reputation and trust
  - Loss of profit
  - Right to compensation
  - Fines from ICO



What does the Act apply to?

- Personal information – data processed that can identify a living individual
- Processing – anything you do with the data!
- Data subjects – the living individuals concerned
- Data controllers – those who process personal data, or have it processed

Personal data – does not cover the deceased. Not corporate information (eg profit and loss accounts, widget production figures etc). Does include info about sole traders, partnerships. PD can be a little as name and address. 'Processed' is a wide term incls obtaining, recording holding, adding, deleting the personal data. Largely relates to computer held information, but also other automated operations like CCTV systems. Certain highly structured paper based records also caught where they constitute a 'relevant filing system' under the Act.

E-context – cookies, profiles, IP addresses

Data Subjects – each and everyone of us. We are all subjects of various databases held by, our employer,bank,local authority, health service etc

Data Controllers – Will include all sizes of legal entity - LTD's, PLC's, partnerships etc. The Act does not differentiate in terms of size

Overview of the DPA

- Sets out eight principles of good information handling, that all data controllers must comply with
- Sets out powers and duties of the Information Commissioner as the regulator
- Requires most data controllers to be added to a public Register (to 'notify')
- Gives rights to individuals (data subjects) in respect of their personal data
- Domestic use is exempt

The Eight Principles

1. Fair and lawful processing
2. Processed for limited & specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than necessary
6. Processed in line with individuals' rights
7. Kept secure
8. Not transferred outside the EEA without adequate protection

Summary of all Principles on this slide. Further details on each follow...

General points on all Principles – broadly drawn, not prescriptive, largely good business practice which orgs would look to implement even if DPA did not exist!!

Do not set hard and fast rules in most cases.

Notification

- Public register of UK data controllers
- Annual notification - £35 fee
- Non-notification (unless exempt) is a criminal offence
- Businesses that process personal information for anything other than *core purposes* need to be registered with ICO
- Not all businesses need to register .... but *all* need to comply with the eight principles

Register is on internet. Broad descriptions of what data controllers do with personal information (ie purposes, type of pd held, disclosures made). Your client details are not put up for all to see!

Insurance industry organisations (large and small) are required to notify – no exemption available

Building in best practice

- Build in privacy considerations at the start
- Only collect what you need
- Only use information for its original purpose
- Only keep information for as long as needed
- Keep it secure, accurate and up-to-date
- "Do-as-you-would-be-done-by"

1 – dotn collect peoples home addresses if you only want to send them an email newsletter

2 – don't use a phone number taken to arrange delivery for market research

3 – have a regular clear out of old information – hoarding old information can be a liability (e.g. old pc's with personal details on just thrown away or put on ebay)

4- make sure it is always secure – don't leave unencrypted memory sticks on the bus or files in cars overnight

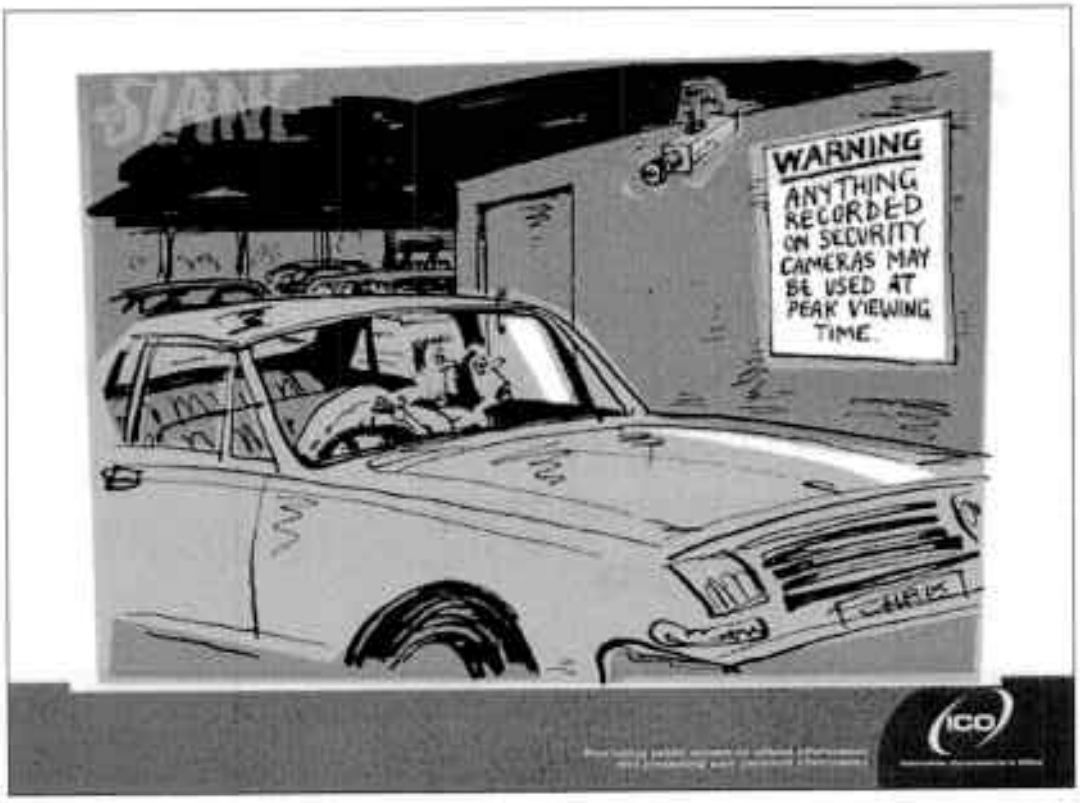
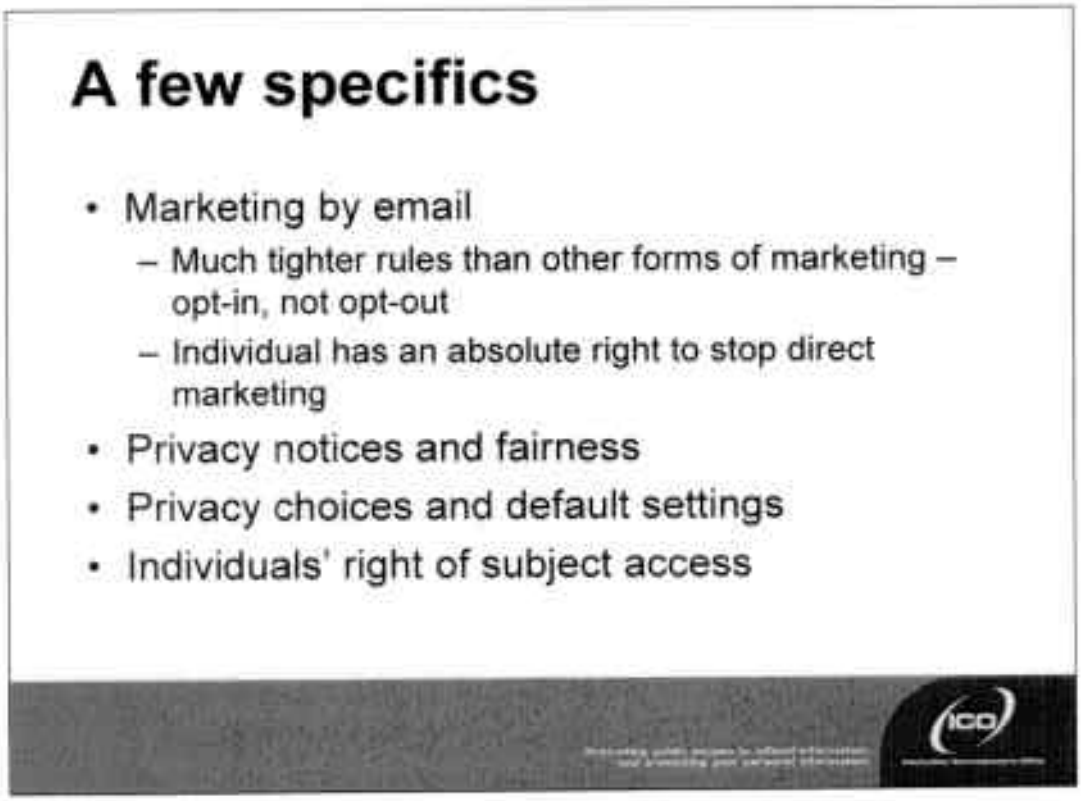


Illustration of fairness / fair processing!

Personal Information Online – new Code of Practice

Contents:-

- Best practice hints and tips
- Marketing your goods and services online
- Privacy choices / default settings
- Operating internationally
- Individuals'rights

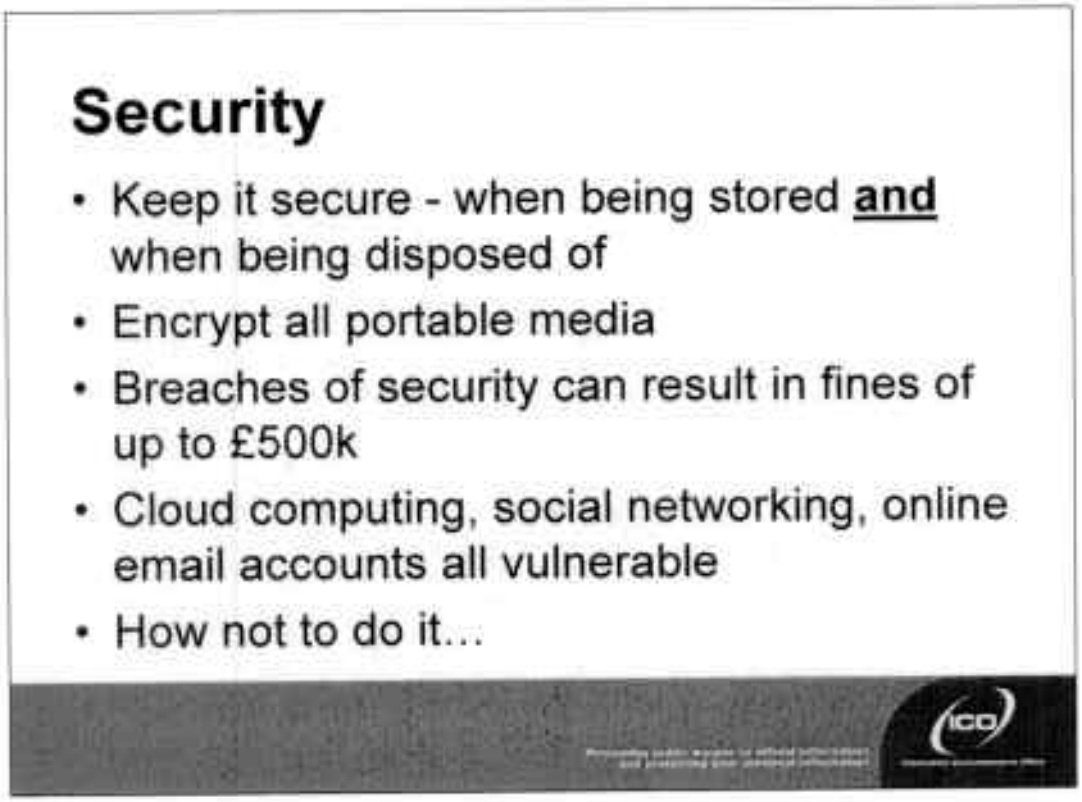


1 - Marketing can be as simple as sending out emails with offers or as complex as behavioural advertising

2 - Individuals have the right to stop and prevent direct marketing under the DPA. Under the first principle you should identify who you are and provide an option to prevent further marketing every time you market someone.

3 - There are special rules covering electronic marketing such as emails, phone and text.

Remember – you have to provide ALL information under these rights, so you may wish to be careful what goes into personnel files and the like!



1 - Securely could mean in lockable cabinets, or using passwords and encryption on computers. You shouldn't put a password into a computer at the beginning of the day, and then let staff have free access to all files on the computer for the rest of the day. If necessary password protect individual documents or databases where personal information are held.

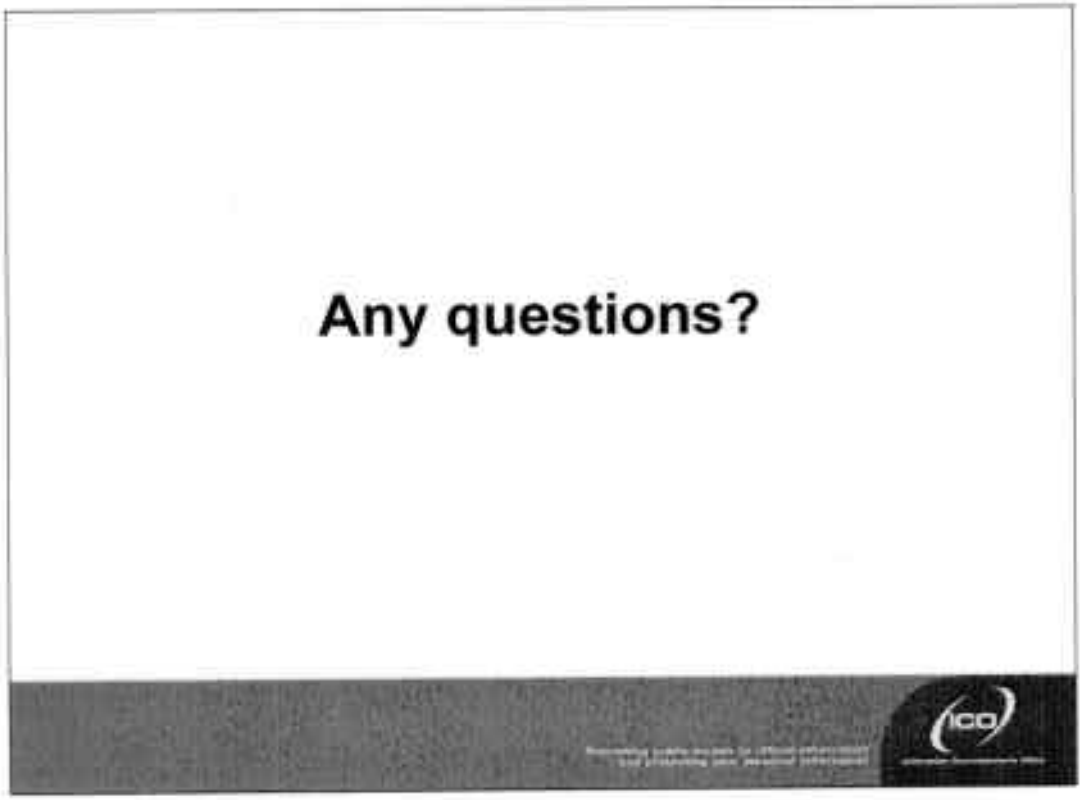
Get the best you can buy!

2 – its no good keeping information under lock and key for years, and then when its no longer useful to you, putting it out with the recycling or leaving files in cabinets going to the dump

3 - There are now severe penalties for breaching the act or carelessly losing information

4 – the online world now makes information vulnerable. You could be unwittingly transferring information abroad by saving photos on myspace or keeping business documents on googledocs.

The weakest link?



WE ARE HERE TO HELP! Please call us if you ever have any queries

Contact us

- Information Commissioner's Office (Wales)
  Cambrian Buildings
  Mount Stuart Square
  Cardiff Bay
  Cardiff
  CF10 5FL
- Website: www.ico.gov.uk
- Telephone: 029 2044 8044


ICO
Information Commissioner's Office
www.ico.gov.uk

Data Protection

Ken Macdonald
Assistant Commissioner (Scotland)

ELBEG Conference
12 March 2010

Contents

ico.

Data Protection
v
Freedom of Information

Data Protection v Freedom of Information

Data Protection

The Data Protection Act 1998

Applies to personal data held by all sectors

Freedom of Information

The Freedom of Information Act 2000
The Freedom of Information (Scotland) Act 2002

Applies to non-personal data in public sector only

ico.

Data Protection v Freedom of Information

The Commissioners

Chris Graham – The Information Commissioner

Kevin Dunion – The Scottish Information Commissioner

ico.

The Data Protection Act
1998

The Data Protection Act 1998

Eight Principles of Data Protection

Fair and lawful processing

Processed for specified purposes

Adequate, relevant & not excessive

Accurate & up to date

Kept no longer than necessary

ico.

The Data Protection Act 1998

Eight Principles of Data Protection (cont'd)

Processed in line with rights

Must be secure

Must not be transferred to countries without adequate protection

ico.

Information Sharing

Conditions for Processing

Personal Data:
(Schedule 2)

Consent

Contract

Legal obligation

Vital interests

Public interest

Legitimate interest of data controller

Sensitive Personal Data:
(Schedule 3)

Explicit consent

Compliance with employment law

Vital interests

Not-for-profit organisation

Information made publicly available

Legal advice

Public functions

Medical purposes

Equal Opps Monitoring

ico.

Information Sharing

To share or not to share ?

Fair and transparent ?

Conditions for processing

Need to share

How much to share

Sharing consistently

ico.

Information Sharing

Sharing Securely

Volume of data

Retention

Systems

Reviews

ico.

Powers & Penalties

Current Powers & Penalties

Breaches

Formal Undertakings
Enforcement Notices
Audits only with consent

ico.

Current Powers & Penalties

Offences

Sec 55 offence
Failure to Notify
Failure to follow Notice
Max £5k in Sheriff Court
Unlimited fine in High Court

ico.

Criminal Justice & Immigration Act 2008

Provisions:

s77 Power to alter penalty for unlawfully obtaining etc. personal data

s78 New defence for purposes of journalism and other special purposes

s144 Power to require data controllers to pay monetary penalty

ico.

Criminal Justice & Immigration Act 2008

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

Maximum Penalty of £500k
Content of Notices of Intent
Content of Monetary Penalty Notice

ico.

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
ICO Guidelines

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.

Coroners & Justice Act 2009

Provisions:

s173 Assessment notices

s174 Data-sharing code of practice

ico.

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

Statutory Code of Practice to follow

ico.

Assessment Notices

ICO will aim for co-operation

Recommendations aimed at helping

Developing capability – staff and audit practice

Question of publication to be addressed

Spot Checks involve publication – but only after a department's response to our recommendations

ico.

Information Sharing Code of Practice

The Commissioner must prepare a code of practice which contains—

practical guidance in relation to the sharing of personal data in accordance with the requirements of the DPA

and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

ico.

Information Sharing Code of Practice

No statutory requirement to follow the code

but

The code will be admissible evidence in court proceedings

and

Failure to abide by it will be taken in account

ico.

Information Sharing Code of Practice

Currently being drafted

Consultation required by statute

Expected publication late summer

ico.

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

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

ico.


ICO
Information Commissioner's Office
www.ico.gov.uk

Data Protection: Implementation of the new powers of the ICO

Dawn Monaghan
Senior Manager ICO

Records Management Conference
March 2010

Background

- Significant losses of personal data
- Existing powers deemed inadequate
- Public calls for criminal offence
- Preferred option was to imposed a monetary penalty

ico.

Legislative Framework

- New power inserted into Section 5 of The Data Protection Act 1998 through section 144 of the Criminal Justice and Immigration Act

- S55A-E of Data Protection Act 1998 comes into force on the 6th April 2010

ico.

New Powers

- Monetary Penalties
- Extended Audit Powers

ico.

Monetary Penalties

- ICO may 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.

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

ico.

Monetary Penalties

- The contravention was of a kind likely to cause substantial damage or substantial distress **and** either…
- The contravention was deliberate **or**,

ico.

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.

Monetary Penalties

Seriousness of contravention

- Nature of personal data involved
- Duration and extent of contravention
- Number of individuals actually or potentially affected
- Matter of public importance – e.g. Security breach

ico.

Monetary Penalties

Contravention was of a kind more likely than not to cause substantial damage or distress to one or more Individual

- Considerable in importance, value, degree, amount or extent
- Not perceived but of real substance
- Damage is financially quantifiable
- Injury to feelings, harm or anxiety suffered by one or more individual

ico.

Monetary Penalties

Contravention was deliberate

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

ico.

Monetary Penalties

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.

Monetary Penalties

Failed to take reasonable steps to prevent the contravention

- Contravention was caused or exacerbated by circumstances outside the control of the data controller
- Data controller has already complied with requirements of another regulatory body
- There was genuine doubt or uncertainty that any relevant conduct, activity or omission was a contravention

ico.

General Approach

- New territory for the ICO and further guidance will be produced on actual precedents

- ICO may still serve an Enforcement Notice

ico.

General Approach

- Only applies to serious contraventions of the data protection principles
- May be wide variations depending on the circumstances of each case
- Financial resources will be a factor

ico.

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 beginning with the first day after date of service

ico.

Monetary Penalty Notice

- ICO must consider any written representations before deciding whether to issue a Monetary Penalty Notice
- ICO may decide to issue a Monetary Penalty Notice requiring a data controller to pay the amount specified
- Alternatively ICO will inform the data controller that no further action will be taken

ico.

Extended DP audit powers

The approach of the ICO

To Date

- Risk based approach to help focus on organisations which might be striving to comply, but where complaints are significant and where intelligence highlights the risk of failure, Normally done on a consensual basis

ico.

Extended DP audit powers

The approach of the ICO

The Future

- Instances where we need to undertake compulsory audits where there is a risk that individuals data will be compromised and the organisation has been unwilling to engage

ico.

Extended DP audit powers

- Extended Powers only presently extend to Government Departments
- Possibly take in other public bodies
- May in the future extend to private companies

ico.

Assessment Notices Code of Practice

- In consultation at present time, closes 24th March
- To be Published next month
- Provides framework for how audits will be conducted and when assessment notices will be served
- Will outline the approach to audit, audit reports and recommendations

ico.

Assessment Notices Code of Practice

Scope

- Sets out Documents and information to be examined or inspected and those which are not
- The nature of the inspections and examinations
- The nature of interviews
- The preparation, issuing and publication of assessment reports

ico.

Assessment Notices Code of Practice

Documents and information to be examined or inspected

- Access will be required to specific documents, such as strategies, policies, procedures, Privacy impact assessments, job descriptions, training materials, guidance etc

ico.

Assessment Notices Code of Practice

Documents and information to be examined or inspected

- Access may also be required to specified personal data, or classes of personal data and to evidence that it is being handled in accordance with policies and procedures

ico.

Code of Practice

Documents and information not to be examined or inspected

- Information subject to legal professional privilege
- Classified 'Top secret'
- Equivalent commercially sensitive information

ico.

Code of Practice

Documents and information not to be examined or inspected

- Manual
- Electronic
- Data stored centrally
- Data stored locally
- Mobile devices and media

ico.

Code of Practice

The nature of the inspections and examinations

- Carried out to indentify objective evidence about the implementation of policies and procedures and how effectively they are mitigating risk

ico.

Code of Practice

Inspections and examinations used to Evaluate how a data controller:

- Stores, Organises, adapts, alters information or personal data
- Retrieves, consults or uses information or personal information
- Discloses personal data by transmitting, disseminating or other means
- Weeds and destroys personal data

ico.

Code of Practice

The nature of interviews

Comprise of discussions with:

- Data controllers staff and contractors
- Data Processors staff
- Staff of relevant service providers as specified in the Assessment Notice

ico.

Code of Practice

The nature of interviews

- Discussions conducted to further develop an understanding of working practices and awareness of data protection considerations
- Departmental managers, operational staff, support staff and staff involved with information governance may be considered for interview

ico.

Code of Practice

The nature of interviews

- Prior to audit discussions will be scheduled of areas to be covered and those to be interviewed will be provided to the data controller
- Individuals will be advised by the data controller in advance of their participation

ico.

Code of Practice

The nature of interviews

- Key control questions will be used to understand roles and processes

- Some questions may relate to data protection training and awareness but will not be framed as a test

ico.

Code of Practice

The nature of interviews

- Interviews maybe conducted at an individuals workstation or in a separate room depending upon circumstances

- Interviews are to help in assessing compliance, they do not form part of or provide information for any disciplinary investigation

ico.

Code of Practice

Preparation, issuing and publication of assessment reports

The findings will be presented by way of;

- An executive Summary
- An audit opinion
- Detailed findings against predefined risks
- Associated recommendations

Code of Practice

Preparation, issuing and publication of assessment reports

- The ICO will take into account opinions of the data controller concerning the suitability for publication of any element of the report.
- Compulsory audit reports will be published on the Commissioners' website for 12 months

ico.

Code of Practice

Preparation, issuing and publication of assessment reports

- May be available on request after 12 months
- The Commissioner may include details of the assessments in his annual report

ico.

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

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

ico.

FASTIIS 25/5/10

Information Commissioner's Office

Data Protection:
Stronger enforcement, greater encouragement

Jonathan Bamford
Head of Strategic Liaison

2010
25th May

Monetary penalties

- Introduced in April 2010
- Criminal Justice and Immigration Act 2008
- Penalty of up to £500,000 for serious breaches, committed knowingly/recklessly
- ICO statutory guidance has been approved by the Secretary of State and laid before Parliament

Amount of Penalty

- Nature of contravention
- Effect of contravention
- Behaviour of Data Controller
- 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

Assessment Notices

- ICO will aim for co-operation
- Recommendations aimed at helping
- Developing capability – staff and audit practice
- Question of publication to be addressed
- Code of Practice out for consultation

Breach Notification

- Voluntary arrangement
- No legal obligation to notify ICO - Yet
- Revised E-Privacy directive signed
- Mandatory breach notification for CSPs
- Adoption within 18 months

1040

Our 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

Some Other Developments

- The Privacy Dividend: The business case for investing in proactive privacy protection
- Personal Information Online Code
- Statutory Code on Information Sharing
- Guidance – Security for SMEs
- Implementation of Revised E-Privacy Directive
- Implementation of EU Lisbon Treaty
- Review of Directive

ICO

Information Commissioner's Office

Sign up to our e-newsletter at www.ico.gov.uk

So carrots & sticks

10 40