Information Commissioner's Office: More enforcement, more encouragement

IRMS, LLandrindod Wells, 24 November 2010

Anne Jones
Assistant Information Commissioner (Wales)

Overview

1. Security breaches
2. New powers – monetary penalties
3. New powers – audit and assessment
4. Other issues

ico.

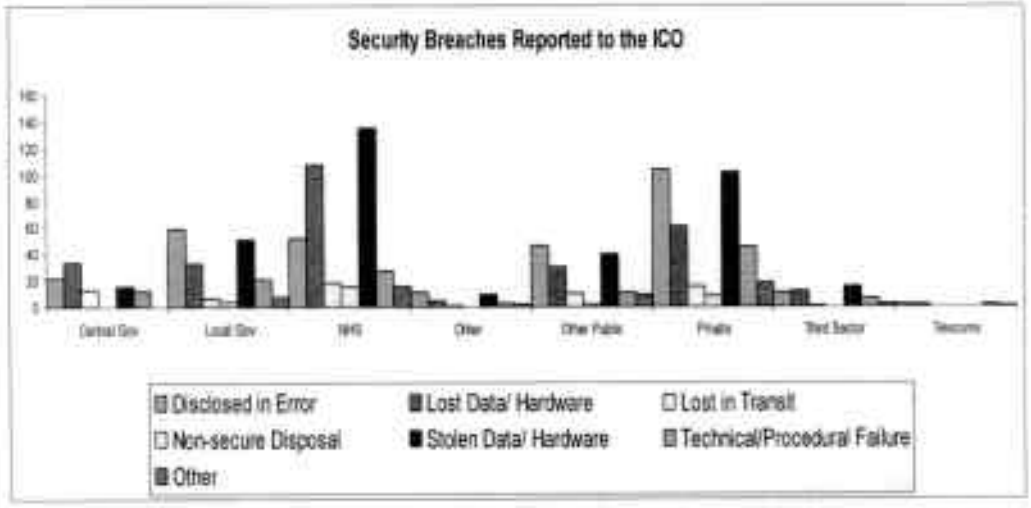
1. Security Breaches – The Problem

ico.

Breaches reported since Nov 07

	Disclosed in error	Lost Data/ Hardware	Lost In Transit	Non-secure Disposal	Stolen Data/ Hardware	Technical/ Procedural failure	Other	Total
Central Gov't	22	34	13		16	12		97
Local Gov't	69	33	8	4	51	21	7	181
NHS	52	108	18	16	135	27	16	372
Other	13	7	1		9	5	2	37
Other Public	47	30	10	2	40	11	9	149
Private	104	61	16	8	102	46	19	355
Third Sector	11	12	1		16	6	3	50
Total	308	285	65	30	369	128	56	1241

ICO.


Security Breaches Reported to the ICO
Disclosed in Error
Lost Data/ Hardware
Lost in Transit
Non-secure Disposal
Stolen Data/ Hardware
Technical/Procedural Failure
Other

ico.


ico.

Some Conclusions

- Data breaches continuing
- Personal information not sufficiently valued
- Theft/loss of portable devices significant
- NHS has particular problems
- Lack of communications/training a frequent factor
- Need to check contractors/processors
- Policies not fit for purpose
- Not just about security

ico.

Lack of accountability

Lack of scrutiny

2. New Powers – Monetary Penalties

- Background
  - Significant losses of personal data in 2007
  - Existing powers deemed inadequate
  - Calls for criminal offence
  - Preferred option was to impose a monetary penalty
- Criminal Justice and Immigration Act 2008: section 144 inserts section 55A-E into DPA 1998
- Introduced on 6 April 2010

ico.

Monetary Penalties (cont.)

- Penalty of up to £500,000 for serious breaches of any of the data protection principles, committed knowingly/recklessly
- Criteria for fines laid down in law
- Financial resources will be a consideration (20% discount if paid within 28 days)
- ICO may still serve an Enforcement Notice (or Undertaking) with the CMP

ico.

This will address the cause of the breach (the CMP doesn't do that)

Specific requirements

- Before imposing a monetary penalty the ICO has to be satisfied under section 55A DPA 1998 that:
- *"There has been a serious contravention of 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.

Specific requirements (cont.)

- *The data controller knew, or ought to have known, that there was a risk that the contravention would occur,*
- ***and** knew 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.

Likely imposition of a Monetary Penalty:-

- Seriousness of contravention
  - Number affected
  - Nature of personal data
  - Duration and extent of contravention
  - Matter of public importance
- Contravention likely to cause substantial damage/distress to one or more individuals
  - Damage is financially quantifiable
  - Injury to feelings, harm or anxiety suffered by one or more individuals

ico.

- Contravention was deliberate, or premeditated
  - Series of similar contraventions and no action taken by data controller to rectify cause of original contraventions
- Knew, or ought to have known
  - Failure to carry out any risk assessment
  - Contravention was, or should have been apparent to a reasonably prudent data controller
- Failed to take reasonable steps to prevent contravention
  - Inadequate procedures and policies
  - No clear lines of accountability
  - Failure to implement ICO etc guidance or CoPs

ico.

Less likely imposition of a Monetary Penalty:-

- Contravention caused by circumstances outside direct 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.

The process

- Notice of Intent setting out the proposed amount of the CMP
- 28 days to provide written representations to the ICO
- Representations considered
- Monetary Penalty Notice issued, OR no further action taken OR proceed by way of Enforcement Notice etc.
- Cases in the pipeline

ico.

3. New Powers – Audit and Assessment

- Audit is key to educating and assisting organisations to meet their obligations
- Organisational benefits of audit:-
  - Independent assurance
  - Identifies risks and mitigations
  - Measures compliance
  - Increases staff DP awareness
  - Can act as a catalyst for change

ico.

•– good practice

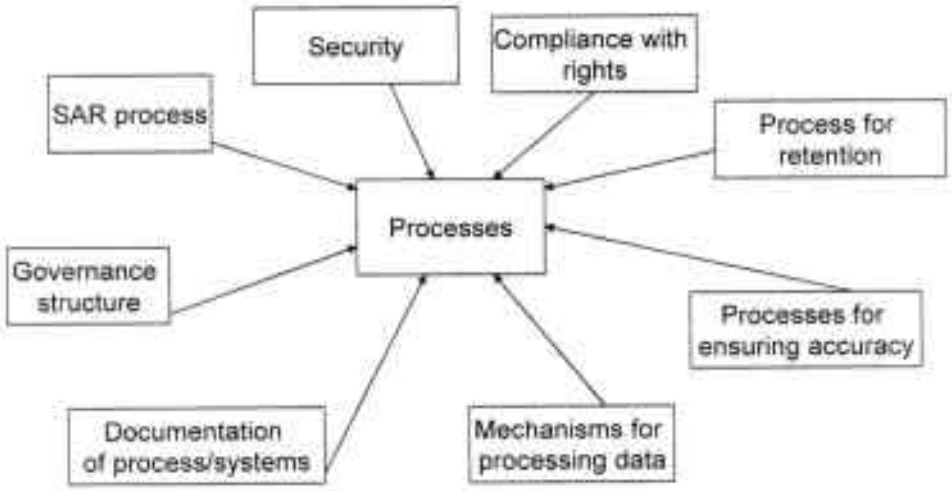
- Coroners and Justice Act 2009: power to audit in the absence of consent...
- ..following issue of an Assessment Notice
- Initially government departments only
- Code of Practice issued
- Assessment Notice will impose specific requirements; Notice and ensuing report to be published
- Preferred strategy: consensual rather than compulsory

ico.

- 11 audits so far this year (since April). Nb they are *free*
- All audits to date have been consensual
- Endeavour to keep the organisational burden to a minimum
- Audits have shown:-
  - Examples of good practice exist
  - Retention/lack of weeding a problem
  - Policies/procedures not related to jobs
  - Some way to go on staff awareness

ico.

Areas we audit



ico.

Current Approach to (Consensual) Audit

- Agree a scope of work with the organisation
- Carry out an off-site check of an organisation's documented policies and procedures
- Carry out an on-site review of the procedures in practice for processing personal data
- Provide a report that indicates whether we consider the organisation's processing is likely or not to comply with the DPA along with recommendations to help them to do so.
- Write an Executive Summary that we can publish on our website, with the consent of the organisation.
- Carry out a follow-up review approximately six months after the audit.

ico.

4. Other issues

- Code of Practice on Information Sharing
- Government's transparency agenda
- New approach to investigating DP complaints
- Report to Parliament on state of surveillance
- E-Privacy Directive
- Review of EU Data Protection Directive
- INSPIRE regulations

ico.

- 2 week consultation commenced 8th October
- Submission to SoS in January
- New Code will:
  - Cover both routine and ad hoc sharing
  - Apply to public and private sector
  - Provide a process for working through data sharing problems
  - Include practical examples
  - Include links to other guidance

Contact us:

Information Commissioner's Office (Wales)
Cambrian Buildings
Mount Stuart Square
Cardiff Bay
Cardiff CF10 5FL
Tel: 029 2044 8044

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

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

ico.

Social marketing, personal privacy: complying with the law

Ken Macdonald
Assistant Commissioner
Information Commissioner's Office

Mackay Hannah Social Media Conference

22 November 2010

Contents

ico.

The ICO

Regulator of

Data Protection Act 1998
Privacy & Electronic Communications Regs (2003)

Freedom of Information Act 2000
Environmental Information Regulations 2004

ico.

The Data Protection Act

The Data Protection Principles

1. Process data fairly and lawfully
2. Processed for one or more specified lawful purposes
3. Ensure data is adequate, relevant and not excessive
4. Ensure data is accurate and kept up to date

ico.

The Data Protection Principles

5. Keep data for no longer than is necessary
6. Process in accordance with people's rights
7. Keep data secure
8. Limit transfers outwith EEA

ico.

Privacy & Electronic Communications Regulations

Application of PECR

Marketing and advertising by electronic means including:

- Telephone
- Fax
- Email
- text message
- picture / video messaging
- automated calling systems

ico.

Application of PECR

Also covers

- use of cookies
- telephone directories
- traffic
- location data.

ico.

Electronic mail

"Any text, voice, sound, or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service"

Much more than e-mail !

ico.

Electronic mail

Unsolicited marketing needs consent

"Soft" opt-in possible

Must include:

- Identity of sender
- How to opt-out

ico.

Electronic mail

Points to consider:

Third party lists

Updating lists

E-mail Tracking (clear gifs/beacons/web bugs)

Viral marketing

ico.

Cookies

Cookies or similar devices must not be used unless the subscriber or user:

•is provided with clear and comprehensive information about the purposes the cookies;

and

•is given the opportunity to refuse them

ico.

Cookies

Exemptions:

Where cookies are for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network;

or

where such storage or access is strictly necessary to provide an information society service requested by the subscriber or user.

ico.

Location

Location data relating to a subscriber or user may only be processed where:

the subscriber or user cannot be identified from that data

or

where it is necessary to provide a value added service with the consent of the relevant user or subscriber.

ico.

Penalties

The ICO as Regulator

Considers likelihood of compliance with DP Principles / Regulations

When necessary, will take enforcement action:

- Undertaking
- Enforcement Notice
- Civil Monetary Penalty (DP only)

ico.

Conclusions

Wide range of data protection issues

Internal compliance important

Getting it wrong can be costly !

ico.

Information Commissioner's Office

93-95 Hanover Street
Edinburgh
EH2 1DJ

0131 301 5071
Scotland@ico.gsi.gov.uk
www.ico.gov.uk

Developing good practice together

Ken Macdonald
Assistant Commissioner
Information Commissioner's Office

Scrutiny Improvement and Better
Regulation Conference

19 November 2010

ico.
Information Commissioner's Office

The ICO

Regulator of

Data Protection Act 1998
Privacy & Electronic Communications Regs (2003)

Freedom of Information Act 2000
Environmental Information Regulations 2004

ico.

The ICO in Scotland

	DP/PECR	FOI/EIR
Public Sector (Reserved Matters)	✓	✓
Public Sector (Devolved Matters)	✓	
Private Sector	✓	
Voluntary Sector	✓	

ico.

Regulation and the DPA

ico.

Regulators and the DPA

Must comply with the data protection principles

but

Potential exemption from subject information provisions

ico.

The Principles

1. Process data fairly and lawfully
2. Processed for one or more specified lawful purposes
3. Ensure data is adequate, relevant and not excessive
4. Ensure data is accurate and kept up to date
5. Keep data for no longer than is necessary
6. Process in accordance with people's rights
7. Keep data secure
8. Limit transfers outwith EEA

ico.

The "Regulatory" Exemption

Personal data processed for the purposes of discharging functions to which this subsection applies *are* ***exempt from the subject information provisions*** in any case *to the extent to which the application of those provisions to the data would be likely to* ***prejudice*** *the proper discharge of those functions.*

ico.

The "Regulatory" Exemption

Regulators are exempt from the Subject Information Provisions

1 - Process data fairly and lawfully

6 - Process in accordance with people's rights

When processing to

- protect members of the public from dishonesty, malpractice, incompetence or seriously improper conduct, or in connection with health and safety;

- protect charities; or to

- promote fair competition in business.

The ICO as Regulator

Considers likelihood of compliance with DP Principles

When necessary, will take enforcement action:

- Undertaking
- Enforcement Notice
- Civil Monetary Penalty

ico.

Working with the ICO

Internally:

DP Awareness Raising

Voluntary DP Audits

Externally:

Promoting Good Practice

Joint Inspections

ico.

Conclusions

Wide range of data protection issues

Internal compliance important

Role in promoting good DP practice

Getting it wrong can be costly !

ico.

Information Commissioner's Office

93-95 Hanover Street
Edinburgh
EH2 1DJ

0131 301 5071
Scotland@ico.gsi.gov.uk
www.ico.gov.uk

What's on the horizon for the ICO?

ACSeS Annual Conference – 18 November 2010

Graham Smith
Deputy Commissioner and Director of FOI

ico.
Information Commissioner's Office

SURVIVAL!

ico.

Context

- Information rights centre stage
- FOI embedded in public sector
- Compliance or culture change?
- Security concerns for personal data
- Government and European agenda

ico.

FOI/EIR

- Greater emphasis on proactive disclosure
- Government's "Transparency Agenda"
- Transparency Board (Cabinet Office)
- Salary information and public expenditure
- Obvious fit with Publication Schemes

ico.

Complaints to ICO 2009/10

- FOI complaints received: 3734 – 20% up
- FOI complaints closed: 4196 – 39% up
- Significant reduction in age of caseload
- 628 formal decision notices
- 161 appeals to Tribunal

ico.

Complaints Issues

- Volumes increasing
- Resources likely to reduce significantly
- Tougher stance on timeliness
- Revised enforcement policy
- Small authorities – parish councils

ico.

Possible amendments to FOI

- Cabinet minutes – ministerial veto
- Communications with the Royal Family
- Reducing the burden – cost/benefit
- A new "right to data"
- Re-use of public sector information

ico.

Possible extension of FOI

- Newly created public authorities
- Privatised/partnership organisations
- Representative organisations
- Impact on EIR
- Geospatial information - INSPIRE

ico.

Tribunal Activity

- First tier and Upper tier
- Paper hearings v oral hearings
- Strike outs and withdrawals
- Costs rulings
- Consent orders

ico.

Data Protection

- Monetary penalties
- Audit powers
- Higher tier notification fee
- Security breaches
- Undertakings and enforcement

ico.

Information Sharing

- Acceptance of legitimate data sharing
- Public administration and citizen benefit
- Balancing advantages with privacy risk
- Importance of transparency
- Public consultation on draft Code of Practice

Other Current Issues

- Relevant government policy changes
- New initiatives – identity management
- MoJ consultation on legislative framework
- EC review of directive
- Safeguarding personal data while achieving greater transparency

ico.

Public/private information

- DP/FOI tension
- Shift in government and societal expectations
- Anonymisation issues
- Does section 40 produce good outcomes?
- International comparisons

ico.

ICO

- Re-organised and re-vitalised
- Integration of DP and FOI work
- Under one roof
- Reviewing reporting relationships – MoJ/Parliament
- Making the best use of available resources

ico.

HERE TO STAY!

ico.

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

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

ico.