

Dr. FSS
18/11

(2010)

Data Protection Issues for Financial Services Firms: The ICO perspective

Jonathan Bamford
Head of Strategic Liaison

Public social concerns

Preventing crime	93%
Protecting personal information	82%
Unemployment	80%
The NHS	80%
Improving education standards	80%
Equal rights for everyone	87%
Protecting freedom of speech	86%
National security	85%
Environmental issues	83%



Financial services complaints to ICO

[illegible]

- 1. loss of weight due to weight increase
 - 2. loss of weight due to weight increase
 - 3. loss of weight due to weight increase
 - 4. loss of weight due to weight increase
 - 5. loss of weight due to weight increase
 - 6. loss of weight due to weight increase
 - 7. loss of weight due to weight increase
 - 8. loss of weight due to weight increase
 - 9. loss of weight due to weight increase
 - 10. loss of weight due to weight increase

- Also it is your 1st time on 21 -
you don't know any because a slot
board puts things in there out with

- New growth for plants & emergence
of adult at same place -
dispersed seed - full tree shelter -
note -

- Why is this, would that body
take water up to have a similar
pressure - is that the case?
- pressure is pushing water up
to give the water a positive pressure
to move and direction of blood
that way.

Get a good working no. on

540-22 p/b 1 & 1 uncl.

KS gone home, Eng gone ✓

P.1 volume cost = 100

Fixed source now of 21
by 1992 - end of 1992

4/Nov 13 str 12 -

→ keep and at appropriate

- your paper has no real value

- refusal law - 1. p. 147

Page 1

- Its high 100 benzene
200 consumed.

Financial services complaints to ICO



ico.

So wide the issues

- but extending over 25 years DfW
where cases reported in place in the
80s largely built for that so they are
about subject areas

Financial services compliance

- ICO relationship with FSA
- Imposition of monetary penalties
- Zurich UK fine £2,275,000
- Risks mitigated by breach notification to FSA and ICO plus other proactive steps
- Fine imposed reflected this

ico.

- FSA has an MIP under FSA Act -
Try to reports - online paper files in the
Not always as well as could be done to move

MP Guidance 3, 4 - if already caught -
then they can be / as a consequence
understand beyond not multiple instances
single failure

ICO will not find time

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

ico.

- People say why not
imposed any year -
well by the process -
ask to give data -
then to respond to
proper penalty - all like
have worked this way

Amount of penalty

- Nature of contravention
- Effect of contravention
- Behaviour of Data Controller
- Impact on Data Controller
- Other Considerations

ico.

Seriousness - how many - number of people affected - impact on users

whether, how, and why issues

of the law - given notice put out to users

way of implementation - need to make examples

- concerned with Director's head and thought tables

search Google could be put about it as to future results

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
- Audit as an enforcement tool - Google

ico.

Our approach

- No 'toothless watchdog', 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.

- Although can strengthen not source of data

- want right in first

why Code of Practice as the

- using P by D -

- principles - general

P by A

Privacy Directive

A range of challenges ahead

- Government's programme on openness, transparency, privacy and information rights
- Transposition of e-Privacy Directive into UK law
- Information sharing code of practice
- Report to Parliament on the state of surveillance
- Report to Parliament on operation of ELMER suspect financial transaction database
- ICO technological expertise and Technology Reference Panel
- Develop the Personal Information Promise
- Possible amendment to OF 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.**

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

Oct 2, Carver, N.D., Hutton.

- Consent to Surgery
- Brain orderlies by CP

On average - Steel rule used
C & J A

~ 19, 10 me

~~Line~~

Strongly Red Oxidation

- Самостоятельно

Not sure, the color
cannot show here yet
- by D Purple L -

So, in summary:

Final series begins

Final K is - strong and end

- total volume percentage
reflected per day

= right side is roots in \mathbb{C}

SA problem

- More generally DP has ~~structure~~ ^{structure} and direction of travel in that dist

- Public museum worth new building

- May 1st removed about 100
or by 2-3 years ~~of age~~

- logarithmic number of hidden units
- existing neurons effective
- n/100 hidden units

~~too old and public~~

No standards at Turkey who try to stay - some nighting
 H/L with all over - best picture who
 are included in the property to be able
 - included in the two day
 - included in the two day
 - included in the two day

Freedom of Information Act: Providing Greater Transparency

Inside Government Civil Liberties Conference – 11 November 2010
Graham Smith
Deputy Commissioner and Director of FOI



Context

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

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

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

Possible extension of FOI

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

Concerns

- Impact of spending review/budget cuts
- Good information handling key to service delivery and citizen empowerment
- Must not be relegated to “back office” function
- Proper safeguards for personal information

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

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

Upholding information rights: Hot topics in a cold climate

Christopher Graham, Information Commissioner



10th NOV 2010


Cold Climate

- Recession
- Public spending cuts
- Front line v back office
- Distrust of authority
- Disillusion and disengagement

Hot topics


- Hanging on to customers
- Transparency and accountability
- Information rights on the front line
- Citizens fight back
- ICO never busier

ico.




Big Brother is
watching you!

ico.




Big Brother is
watching you!




Big Brother
has stolen
your identity!


ico.



Big Brother is
watching you!

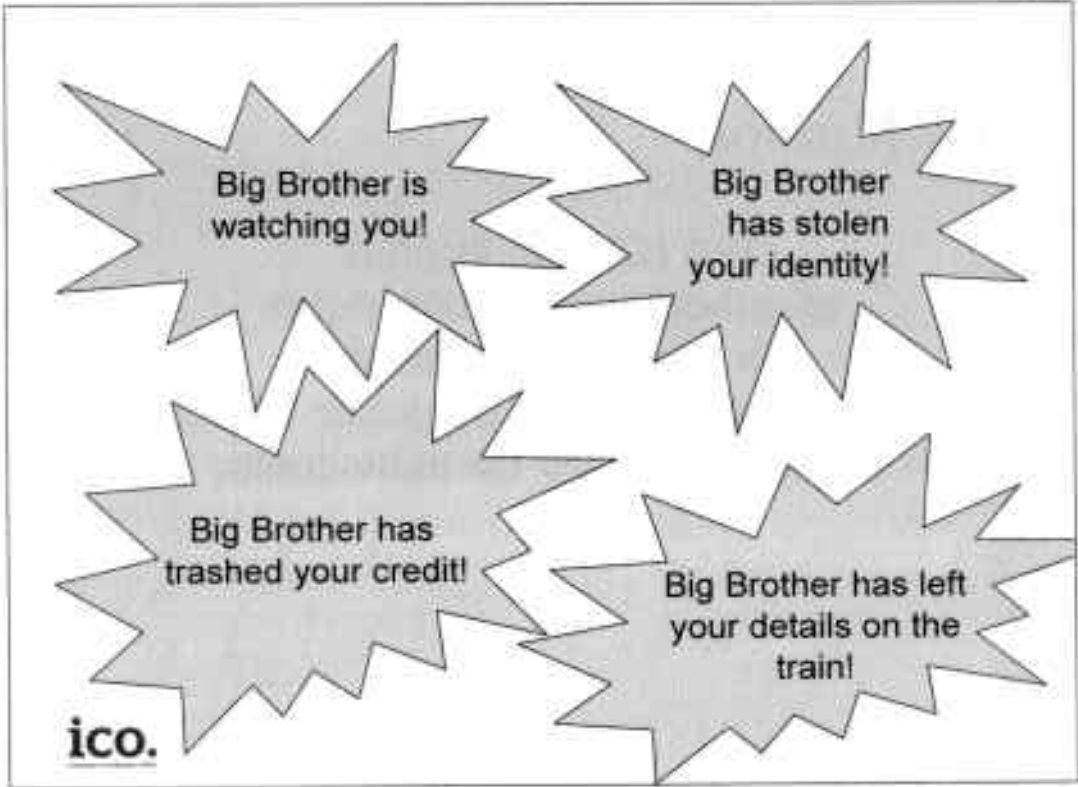


Big Brother
has stolen
your identity!



Big Brother has
trashed your credit!

ico.



Big Brother is
watching you!

Big Brother
has stolen
your identity!

Big Brother has
trashed your credit!

Big Brother has left
your details on the
train!

ico.

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.

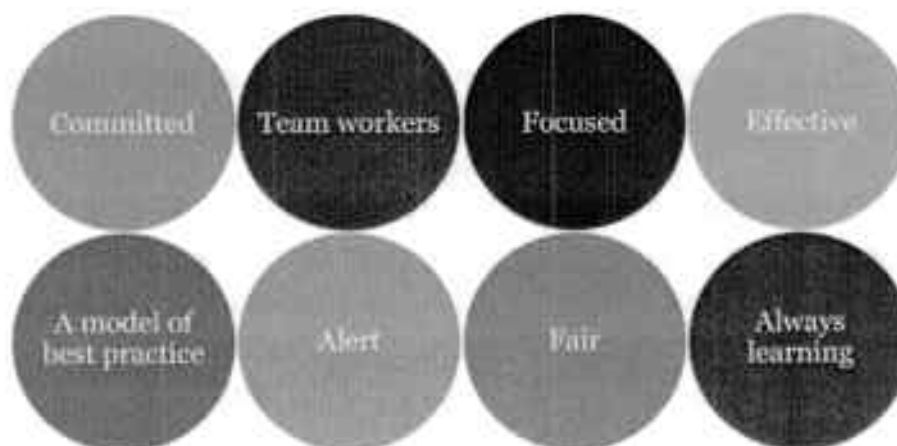
ico.

Our Vision

By 2012, we will be recognised by our stakeholders
as the authoritative arbiter of information rights,
delivering high-quality,
relevant and timely outcomes,
responsive and outward-looking in our approach,
and with committed and high-performing staff
- a model of good regulation,
and a great place to work and develop.

ico.

Our values



ico.

We are:

Committed

We care about upholding information rights

Team workers

We work together as one ICO team, sharing information and expertise

Focused

We give priority to activities that make the biggest contribution to achieving our mission

Effective

We work productively and efficiently to produce high quality and timely outcomes, offering best value for customers and citizens

A model of best practice

We do not ask others to do what we are not prepared to do ourselves

Alert

We are alert to the perspectives and needs of all our stakeholders - and to the potential impact of new developments in our business

Fair

We treat everybody we deal with fairly and with integrity and respect. We are inclusive in our approach

Always learning

We are always learning and developing professionally

Coalition priorities

What we do is where it's at

- Accountability
- Transparency
- Freedom
- Privacy

Efficiency

- Accountability drives savings
- Transparency identifies waste
- Right first time
 - Proactive disclosure and 'privacy by design' are cheaper

ico.

PRESS NOTICE

Data sharing COP consultation would be good I think – it launches this Friday and your talk would be a chance to show we're keen to take a pragmatic approach, to position ourselves as the authority and that we're taking the lead. It's useful to show we're not a hindrance to sensible data sharing.

Powers

- New powers introduced April 2010
 - Power of audit in the absence of consent
 - Government departments – but could be extended to other public bodies and private sector
 - Code of Practice published
- More on the way?
 - Implementing PECR
 - Compulsory breach notification

ico.

There's not a lot that I can add to the suggestions of others. The only thing is that you might follow on from cookies and consent to say something more about the BIS consultation and in particular that the first compulsory breach notification is on the way, albeit confined to communication service providers. Also that implementation of the PECR Directive will require some increase in our powers (we think) but just how much is still under discussion.

Penalties

- Civil Monetary Penalties introduced April 2010
- Penalty of up to £500,000 for serious breaches committed knowingly/negligently
- ICO statutory guidance available
- Amount depends on nature/effect of contravention, behaviour of/impact on data controller
- Watch this space

ico.

People

- Human factor
- Policies → Processes → People
- Human error
- Rogue activity
- S.55 offences

ico.

Personal information online

- Code of Practice
- How the DPA applies to information processed online
- Marketing goods and services online
- Privacy choices
- Operating internationally
- Individuals' rights online
- Things to avoid

ico.

Data sharing code consultation

- 'Walk through' practical guidance and examples
- Public, private and third sectors
- Strong on transparency – esp. FoI
- Clear explanation of 'other law' + DPA
- Strong on 'nuts and bolts' issues
- A 'proper' statutory code: admissible in proceedings
- Consultation ends January 5 2011 – please participate

ico.

Information Security and Identity Management in the Public Sector: Keeping within the law

Christopher Graham
Information Commissioner



3rd Nov 2010

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.

Our Vision

By 2012, we will be recognised by our stakeholders
as the authoritative arbiter of information rights,
delivering high-quality,
relevant and timely outcomes,
responsive and outward-looking in our approach,
and with committed and high-performing staff
- a model of good regulation,
and a great place to work and develop.

ico.

Our values



ico.

We are:

Committed

We care about upholding information rights

Team workers

We work together as one ICO team, sharing information and expertise

Focused

We give priority to activities that make the biggest contribution to achieving our mission

Effective

We work productively and efficiently to produce high quality and timely outcomes, offering best value for customers and citizens

A model of best practice

We do not ask others to do what we are not prepared to do ourselves

Alert

We are alert to the perspectives and needs of all our stakeholders - and to the potential impact of new developments in our business

Fair

We treat everybody we deal with fairly and with integrity and respect. We are inclusive in our approach

Always learning

We are always learning and developing professionally

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

ico.

Public social concerns

Preventing crime	96%
<i>Protecting personal information</i>	94%
Unemployment	93%
The NHS	90%
National security	90%
Environmental issues	90%
Equal rights for everyone	89%
Improving education standards	89%

ico.

DPA security requirements

- Must take appropriate technical and organisational measures taking account of:
 - nature of data and potential harm
 - state of technological development and cost
- Ensure the reliability of employees with access
- Ensure processors give security guarantees
- Penalties of up to £500k can be imposed
- Criminal offence committed if personal data obtained or disclosed without consent of data controller

ico.

Security: more than just technical

- Safeguards have not kept pace with increased information risk
- Lessons from HMRC and MoD data security breaches point as much to cultural and human factors as technical ones
- Information governance and its role in setting organisational culture is crucial
- This has been recognised by many and tools developed to address this
 - ICO: Personal Information Promise
 - Govt: Information Charters
 - IAAC: person centric identity assurance
 - BCS: Data Governance Code

ico.

No single silver bullet!

- Understanding responsibilities
- Practical tools to help compliance
- Privacy by Design
 - aimed at minimising risk
 - includes better identity management
- Governance
- Organisational culture
- Effective enforcement

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
 - eg NHS Trusts

ico.

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

ico.

Amount of Penalty

- Nature of contravention
- Effect of contravention
- Behaviour of Data Controller
- Impact on Data Controller
- Other Considerations

ico.

Assessment Notices.

The Information Commissioner also has a duty under section 51 of the Act to promote the following of good practice among data controllers and to perform his statutory functions in a way that promotes compliance with the Act by data controllers.

Under section 51(7) of the Act the Information Commissioner may, with the consent of a data controller, assess their processing of personal information for the following of good practice.

ico.

Assessment Notices.

Under section 41A of the Act the Information Commissioner may serve certain data controllers with a notice (in the Act referred to as an 'assessment notice') imposing specific requirements on the data controller.

The 'assessment notice' is for the purpose of enabling the Information Commissioner to determine whether the data controller has complied or is complying with the data protection principles. This process will be referred to as a 'compulsory' audit.

ico.

Assessment Notices.

Data controllers covered by section 41A include government departments, designated public authorities and other categories of designated persons.

Any designations will be made by an order made by the Secretary of State.

At present only applies to government departments.

ico.

Main features

- ICO may serve a Monetary Penalty Notice on a data controller requiring payment of a Monetary Penalty which must not exceed £500,000
- Applies to all data controllers in the private, public and voluntary sectors except Crown Estate Commissioners or a person who is a data controller by virtue of section 63(3) DPA 1998-Royal Household

ico.

Specific requirements

- Before the ICO can impose a Monetary Penalty it 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...

Specific requirements (contd.)

- 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.

General approach

- Only applies to serious contraventions of data protection principles
- May be wide variations depending on the circumstances of each case
- Financial resources will be a factor
- New territory for the ICO and further guidance will be produced based on actual precedents
- ICO may still serve an Enforcement Notice

ico.
Information Commissioner's Office

Factors making imposition of a Monetary Penalty more likely

- **Seriousness of contravention**
- Nature of personal data involved
- Duration and extent of contravention
- Number of individuals actually or potentially affected by the contravention
- Matter of public importance
- Example – security breach

ico.

Factors making imposition of a Monetary Penalty more likely

- **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.

Factors making imposition of a Monetary Penalty more likely

- **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.

Factors making imposition of a Monetary Penalty more likely

- **Knew or ought to have known**
- Contravention was or should have been apparent to a reasonably prudent data controller
- Failure to carry out any risk assessment
- No evidence that data controller recognised risks of handling personal data
- Cavalier approach to compliance

ico.
Information Commissioner's Office

Factors making imposition of a Monetary Penalty more likely

- **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
- Not exhaustive

ico.

Factors making imposition of a Monetary Penalty less likely

- Contravention was caused or exacerbated by circumstances outside direct control of 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

Next steps – Notice of Intent

- ICO must serve a data controller with a Notice of Intent setting out the proposed amount
- Notice of Intent must 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

Next steps – 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 data controller that no further action will be taken

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

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

ico.

The new powers of the ICO

IHRIM

November 2010

Dawn Monaghan, Group Manager Public Services



New powers of the ICO - Background

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

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 came into force on the 6th April 2010

New Powers

- Monetary Penalties
- Extended Audit Powers

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

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

Monetary Penalties

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

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

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

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.

Information Commissioner's Office

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.

Information Commissioner's Office

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

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

General Approach

- New territory for the ICO and further guidance will be produced on actual precedents
- ICO may still serve an Enforcement Notice

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 beginning with the first day after date of service

What Happens?:

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

Summary

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

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

Extended DP audit powers

The approach of the ICO – Gov departments

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

Extended DP audit powers

The approach of the ICO – Consensual Audits

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, done on a consensual basis

Audit Powers

- How to request an audit?
- What it would cover?
- How it would be carried out?

Can all be accessed on our website **www.ICO.gov.uk**
under the headings:

Data Protection

For organisations

What is an audit and how can I request one.

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

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