

Intake (4/2)

3.1 DP in PS (inv. 16/6/10)

- Cleve Jones
 - Jackie Clegg

- J6 str ~ 25yo → long-term at DP home
+ home care plan after
J7 home ~ 25 years - CDD - ID (as)
seen DP = Prng + Re prn solutions -
family as as an elected issue
from HSLW members to the local Deaf
state to self advocate (CDD) to p-L
citizen not state in control of the
present situation

- why seen this you change -

- Finally takes up any one of two roles in
the place - our previous personal definitions
Vulnerable
 - Vulnerable to be exploited - outward
 - vulnerable to being exploited -
but often know how
 - vulnerable to something direct
and lessening care.

Not just high profile databases
Hacker/MODP clearly drop - ~~Facebook~~
Instagram - P.V. review came on
to this - lots was CCTV - other related
area, proxy settings on facebook
Google, the entire company with related
accounts.

- However there needs to be a database of stock options and positions, needed
child may need to copy and paste
from - need to update up
 - Penalty for late Dec 1st
~~2015 INFLATERS~~ - due later
from 100 days been a very new website
and still is a concern - not
enough Dec 1st to make 100 per
enough to make Dec 1st to make 100 per
enough to make Dec 1st to make 100 per

From April 1 to power to replace M.L. up to
stock - Feds say a lot more about
this. But it may concern
several weeks as does so many other
things up to 500K - issue M.L. will
be playing now judge!

Jackie says more about what might be
coming (mostly at D) b-r you
know of what takes into great
consideration

Digitized by srujanika@gmail.com

~~1010~~ 1640

Know largely
Private sector
and local government - Local
authorities

— One year since DPA came
into force - now covers all
regulated entities

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

Published April

Breach Notification

Society

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

(a)

— One year since DPA came
into force - now covers all
regulated entities

- None received - some do, no
- At present only Govt Dept & Police
but govt can extend to wider public
and private sector
- Justice Show you a slide where
Answers show you a slide where
Answers show NHS trusts

— Always aim for co-operation and co-creation
- prior to audit approach to determine what

- Compliance history
- Current and DCI highlight technical fail
- Business context - previous issues
- Stakeholders involved and who did what
- Our audit report
- New process / procedure required
- What can bring it in
- What areas of PDS
- Different areas do
- Impact on individuals - 10 - 1000
- no offence
- sentence
- compensation
- disclosure
- damages
- Adjustments periods off
- Give not to publish but to rep
- Not required if DPA activity
or general or other

1 year website - 1,000 or more
New to UK about switching to
new news pub
is a code - (as) No code on
spying - this how do - AJG
- proposed
- public / consumer

Don't go with legal consequences
breaches notification very costly. 100 -
Above voluntary agreement -
likely to have little - One 100
fine and stop you

- But is a code due to based
- On E-Privacy Directive regulation

Has been seen partly - implemented
within UK - very little written
so far.

So sticks have been made bigger
- but wanting to comply with
 place

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

Some Other Developments

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

• Most active



aim to provide tools - but
 need to be left to others
 must be effective
 review those who do not - an
 effective penalties for those who don't

build in due date on
 process - PIA
 harm - PGI
 info - source - SI, by - govt
 FfW - Data sharing - one 1000+

new law in

Published July 2003
Data Protection
Regulation

medium

Collecting policies - new
 (current - P6-9D)

→ So carrots and sticks -

- with cue cards

giving those who look after
 their papers - incentive
 to improve

- where public bodies are responsible
 for the quality of the personal
 information they are holding
 and they are doing something
 to improve it
 inspect include regulators, inc
 and making rules too.

- inspire him, to take public
 and the more penal action
 in some laws.

(O) (D) TV

JB etc

been involved in DfT 23 years -
DfT law became central to regulations (CCTV) -
mainly by accident then spook design had
intended space for CCTV but was overruled
because regulators were not part of culture
CCTV was for purpose - its rules and
standards apply -

- Seen nature of CCTV change
from being a passive reactive eye
to something more active
monitoring capability
- such as ANPR law changes
- big changes in technology - digital
and mobile - body worn, flying
CCTV
- Increasing law making
surveillance a modern after
age crime control as
public safety
- challenge for ICO and
challenge for those who own
to manage CCTV -

ICO perspective: managing your CCTV

Jonathan Bamford
Head of Strategic Liaison



Sept 2010

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



CCTV and information rights

- Images of individuals are covered by the DPA 1998
- The DPA sets legally enforceable standards (data protection principles)
- A DPA code of practice sets good practice standards to help comply with the law
- ICO research shows that the public broadly support CCTV with caveats
- Public authorities have to comply with full laws including providing information on their use of CCTV



bring DfT law to life in
sector

Local Govt CCTV -

JB etc.

Over b/w 25,000 DP law, raising
central to regulation to CCTV
no because spec areas to regulate it
but because it applies to info held about individuals
that include images of them in databases

- seen increasing number and interest in CCTV technology & use in practice - in way DP regulates it etc.
- CCTV changes from being a passive receptacle only - to something that will have more proactive monitoring capabilities - ANPR
- changes in technology - digital and flying CCTV - Body worn
- increases public, media and political interest - reputation as an enforcement body -唐纳德·特朗普 - Bent or new court cases
- question now being begged if or DP + HR + RPA are sufficient to regulate
- challenge for ICO
 - increased use for location cameras etc
 - new and standard DPIT
 - got new power to impose penalties £500k
 - but still about getting right in place

Our intention to regulate CCTV

CCTV and information rights

- Images of individuals are covered by the DPA 1998
- The DPA sets legally enforceable standards (data protection principles)
- A DPA code of practice sets good practice standards to help comply with the law
- ICO research shows that the public broadly support CCTV with caveats
- Public authorities have to comply with FOI laws including providing information on their use of CCTV

ICO.

Breach points not seen passing over papers

proactive due to
complaints (local etc)

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.

HRA

not fucking creepy

Important points

- Is CCTV justified?
- What do individuals expect?
- What is collected?
- Restrictions on use/disclosure
- Image quality
- Retention
- Security
- FOI disclosure:
 - of images
 - of information about use

ico.

Art 8

- impact assessment
- value added review
- controls issue

Sign off / regulatory or
trading board / ANPR

not use chapter

control issue

Under review / initial contact
- travel operators - travel
(DGA)

Industry issue - don't get caught
on any vulnerable legislation

Current issues

- Are we hard wiring surveillance into society?
- Increased use of ANPR
- Blurring of public/private sector interests
- Are existing general laws good enough to provide effective regulation?
- Government's transparency and privacy agenda
- Review of DP legal framework

ico.

licency / schools,

body builder

Private sector benefits - difficult
- our interests

for minors and will break right

Under review of

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

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

- 10.

So been changes and will
be changes as per need of system
but no original one

All say that no longer an
unquestioning approach to value.
No longer acceptable to myself nor
because pupils, affordable & achievable

Gorbachev wants to maximize transparency
of public policies and enhance
privileges of citizens with probabilities
freedom of choice.

- Effortless and unpredictable
at CECU going to be "objectified"
curves going to wind over waves
forces - "impacting public health and
medicine" is now an outcome
that is going to be left to chance
taken for granted or worse still
left to chance.

JB de

Regulation, culture and the surveillance society

Jonathan Bamford
Head of Strategic Liaison



Sept 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.



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



- 25 years - 1st time seen public puts emphasis on individual rights for who want to sue over a侵犯
or privacy
- ~~its first~~ soon politicians, media and members of public call for why
rights are so essential to individuals
and society
- Have seen growing calls to government
put pressure on greater transparency and
local accountability, and good privacy
and data protection codes as
a central element of our work
programme.

- focus added to individual R (now
↳ is pretty big role - not
certain where to start - so start
closer to home - G, r M, -)

- not transparency at all (G, -)
- not privacy at all (G, -)

Although increased
using DP - still
organisational
GP.

1345

1

Data protection: individuals

ico.

Public social concerns

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

ico.

Freedom of information: individuals

ico.

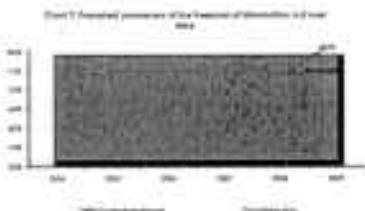
Does any one care
about these inbuilt rights?
- Only paying at the
or relevant to pay for like

- Are these - does
reflect concern - see
many go up in hol
few goes

2

1365

Awareness of the Freedom of Information Act

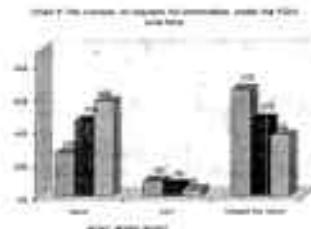


ico.

Freedom of information: organisations

ico.

Information requests



ico.

- Also public money spent
at fol rights - arbella

- Soon fol - maintain
standards or increasingly
will feel it's not
worth to stay.

Surveillance: dataveillance



Surveillance / dataveillance

- Electronic footprints
- Transactions tracked, interactions identified, preferences profiled
- Retained, shared, disseminated
- Increasingly detailed and potentially intrusive picture of our lives

ico.

Database state?

- ContactPoint
- National DNA Database
- Communications data-interception modernisation programme
- National ANPR data centre
- National Identity Register
- E-Borders programme

ico.

- *plus more*

- Sur. Much more direct
CCTV or more obvious
Surveillance technologies - See
growth cult. 'data mining'

- click mouse here will be
an ATM screen
*use of a mobile phone, jones
first ANPR off road car*
- Made 110 verbal debts -> 2006
7 pol officers and issue
of rolling back database state
now a political number

Govt already started
on the database +
some of these - no
surveillance at all on
1 in 3 citizens

-not just public sector

Private sector dataveillance?

- On line services
- Communication services
- Behavioural advertising
- Loyalty cards
- Financial data
- Social networking
- ID scanning

ico.

increased online
pure, locate data etc

Hardwiring surveillance into society?

- Biometric border control
- Aviation security
- CCTV and ANPR
- Surveillance required by licensing conditions

ico.

FP Team Five?

DNR - baby scans

ANPR - number plate
private sec

rot 1 in pbs

Compliance: achieving it in practice

ico.

No single silver bullet!

- Understanding responsibilities
- Practical tools to help compliance
- Effective enforcement
- Privacy by Design
- Governance
- Organisational culture

ico.

INSURG (A) - do as you want

new penalties for non-compliance
For DP
Lessons from DataCom
Sir Ed Bush - M.D.
HMC

Reputation and regulation: matters for the Board

Governance and Accountability

```

graph TD
    GA[Governance and Accountability] --> P[Polices, Procedures, Contracts, Committees]
    GA --> T[Technology - Systems Architecture]
    GA --> Pp[People]
    
```

ico.

Board level issue

The Personal Information Promise

- A chance to regain public trust and confidence by showing senior level commitment
- Not a regulatory compliance tool
- Opened for signature on European Data Protection Day (28 January 2009)
- Signatories from all sectors

ico.

Cop of note on Commitment
in DP reg.

PIP from Volpinne, Royal Mail
BT, Virgin, police force,
Concord, lafarge

ICO Privacy by Design initiative

- Increasing amounts of personal information, increasing risks to individuals
- Technology used in innovative ways to exploit personal information but not always to protect it
- Technological and procedural safeguards have lagged behind
- Better to build in protection rather than bolt on

ico.

- Need to fit culture to respect privacy - needs to be a feature, not a useful

- Identifies Risk overshopped safeguards

- My busy 25m. paper
ready. L - Need a what
project has an budget con.

ICO Privacy By Design work

- Building in not bolting on
- Tools to help:
 - Privacy Impact Assessment Handbook
 - Promoting privacy enhancing technologies
 - Codes of practice/guidance
 - Information governance
 - Business case for investing in privacy protection- "the privacy dividend"

ico.

→ Idea - data management
- IND CONTROL
→ PN, Info slay.

The Privacy Dividend

- Protecting personal information makes good business sense.
- It brings real and significant benefits that far outweigh the effort privacy protection requires.
- Ignoring privacy and not protecting personal information has significant downsides.

ico.

Case appeals to
CFO rather than CEO,

Benefits of protecting privacy

- Organisation earns and deserves trust of individuals. Pays dividends in their loyalty
- More likely to have effective, well run information systems and processes
- Strengthens it operationally and improves resilience.
- Operates with lower levels of risk
- Confident it complies with the law

ico.

More good business sense
not just reputational value

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.

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.

The future: what lies ahead?

ico.

A Range of Challenges

- 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
- Developing the Personal Information Promise
- Possible amendment to DP legislative framework in UK and EU

ico.

Transp. law, Justice, POI, NDAD
Regulation, ATJ, Hostile surveillance
Simpl. P. I., NLR, General Data Protection
Regulation, NLR, General Data Protection

Consent to cookies - break when

The Data Protection Legislative Framework

The Ministry of Justice is running a call for evidence on the current data protection legislative framework.

The Information Commissioner has welcomed the Ministry of Justice's call for evidence on the current data protection legislative framework.

He has no doubt that this framework, which includes the UK Data Protection Act and EU Data Protection Directive, can be improved so that it is more effective in practice, giving individuals an improved set of rights and protections whilst providing greater clarity and reducing unnecessary burdens for data controllers.

ico.

9

1345

The Information Commissioner's view:

- 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.
- The law must provide greater clarity about what is personal data, with a more contextual approach to the sensitivity of information.
- The law must be clearer about when consent is needed and what this involves.

ico.

- built in user bolt or

is going to need other wider controls
as not just user consent, but also

consent not come all at once
relevant - how many times

The Information Commissioner's view:

- The approach the law takes to the responsibilities of the data controllers and processors should better reflect modern business relationships.
- The law needs more realistic rules for international data flows.
- 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.

ico.

May different relationship w/ same
party

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

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

ico.

1-1 conclusion

- No signs statutory or repeat
regulation transparency - thus
patent - largely no
orders and dependency.

- Culture need, to change
it reflects societal views/politic
means

- Can't be an ultimate option
to info public relations - Need
to its consequences address
it reflects, is secure enough
accompanied by stringent data
access rules

10

(Institutional register and often
against local cultures and if
no standard cultures and citizens)

18/05

The Insider Threat - The Forgotten Governance Perspective

Jonathan Bamford
Head of Strategic Liaison

Sept 2010

RSA Europe



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

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

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

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

ico.

Improving Information Governance in the NHS

Jonathan Bamford
Head of Strategic Liaison



Sept 2010

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



Public social concerns

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



OB etc

- it's an old Chinese curse about living in interesting times.
Well we certainly are, 25 years
since seen public relations
in Manchester, and now will be
more to public services
- never seen public relations
subjected on to such vulnerable
aspects to interact
- None govt bodies now gets
any coverage because people
about newspapers are focusing at the
moment on it - too much attention,
citizens control, really bad state
of state - largely been replaced
by business culture
- (O, reads with 10 lines)
 - changed focus
 - still need to get right

- Public and concerned.

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.

rules since 1988 all which
and systems of the
systems, built with controls
with these requirements in mind

functions - can delete! - self
- Not forgotten in time by
Security

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

ico.

Know to talk back's article
1/4 of all deals from NHS Wales
data losses - no answer.
- self or what's best, no
answer

Encryption at particle level
and media

real security - 100% (grade) answer
Human - memory
- culture

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'
- Can't be left to chance

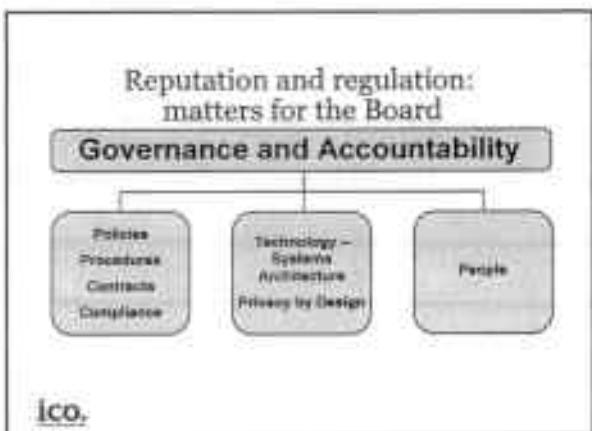
ico.

leadership/culture

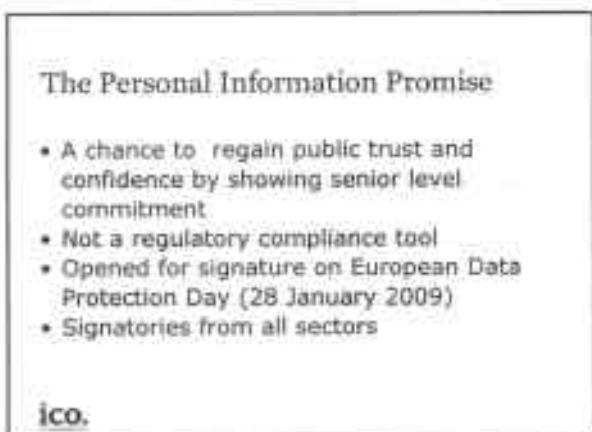
- Microsoft and many others have
- Facebook events highlighted a
culture

- Biggest lesson - not all about
encryption at the

CFO involved

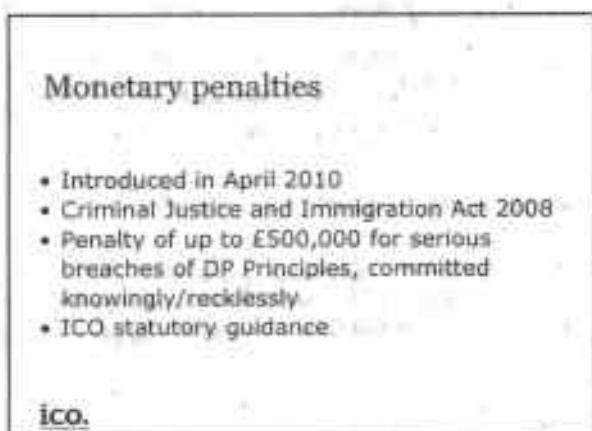


Board level
- rules



- Voluntary BT, by draft
- Vision, LAs, Police Forces
- Trust PCT, ; law firms
Nextar.

Work to get done



Amount of Penalty

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

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.

Future challenges

- Government's programme on openness, transparency, privacy and information rights
- "Liberating the NHS" agenda
 - Greater transparency and patient control
 - Information governance arrangements?
 - Ensuring compliance
- Information sharing code of practice
- Possible amendment to DP legislative framework in UK and EU

ico.

Transparency - location, controllers
Citizens -> request
- NDVAQ (data risk), NIR, CCTV &
changes in place
- what's next to tell? (on
what)
cyber, how about GP access at
home, to medical emergency
smarter - not left to chance

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

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

ico.

- ~~The right about patients~~
- Healthcare info is stored
 - ~~the most sensitive categories
in personal information~~
- Health sector has limited approach
need to keep information other
and secure
- But, important role of blurring
national approaches
- Need to be able to do
- Need to respond to do
- Need to ensure that public
sector and industry (in those
who hold the personal details)
is informed and involved

The ICO: Shaping up to the challenges in the year ahead

Jonathan Bamford
Head of Strategic Planning



Sept 2010

A year of big changes at the ICO



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.

DP Forum 7/1

- 1 year into being
- range of vs.
- new for 1/10
- policy needs
- new role
- other issues
- vs. CAA
- Jumbo
- vs. PIAA

JB dn - 25 years later
4 - 2 years DP has - 3 yrs

- for law
- 3 days off title

~~- 2009 budget changes / change~~

- Committee - now PIAA rather than DPA
~~new budget~~

- 50% - offloading data

- Reviewing existing powers into PIAA
- public sector -

4 changes in progress

- One off power changes at the moment
- change of roles etc or changes to
reflect on other for we have seen challenges
- hold on further update early

- what do we do with

- where were we before the changeover

- where we need to go now

This time last year what CG was doing
spent 1st part of my year ~~refining~~,
~~reorganising~~ - reviews
- responses
- reorganisation

- Making sure we are in shape
for the challenges ahead, taking
the same sorts of changes as you've often
seen in 2010

- Big Reorganisation reflecting
how offfice work

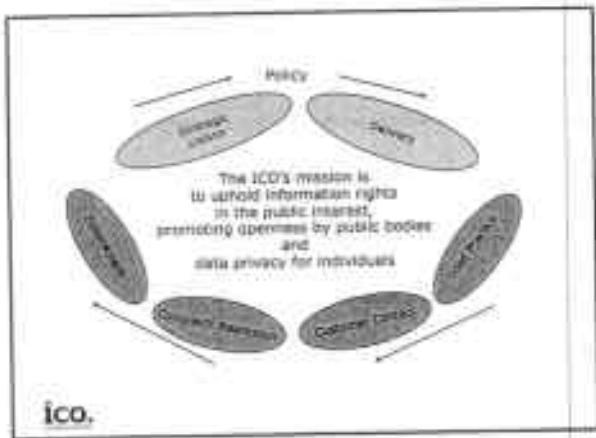
- How we have grown

- And our new powers

- Big message - separate
DPOfSI function to our joint
offfice

Our Mission reflects this

joined up approach to
information rights



Main business units -

Policy and Ops

- lot of cross office working

e.g. dp function b)

bys ec.

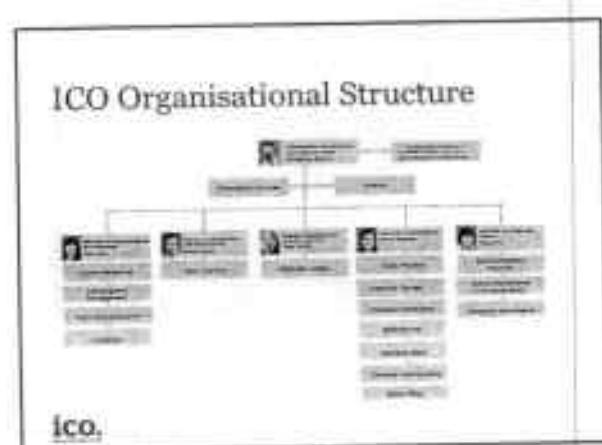
- By Policy Delivery

Split into sub groups
of func

How agencies getters it
how now organised

Don't be confused about what

You are



Strategic Liaison Role

- Maintain and build key relationships and on key issues
- Support and advise key stakeholders
- Promote ICO information rights objectives
- Anticipate change
- Reduce risks

ico.

The Information Commissioner's view:

- 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.
- The law must provide greater clarity about what is personal data, with a more contextual approach to the sensitivity of information.
- The law must be clearer about when consent is needed and what this involves.

ico.

The Information Commissioner's view:

- The approach the law takes to the responsibilities of the data controllers and processors should better reflect modern business relationships.
- The law needs more realistic rules for international data flows.
- 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.

ico.

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

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

ico.

Oversight view

- P's sound but doesn't add much value - PbyD principle
- P's sound but don't add much value - PbyD principle
- P's sound but don't add much value - PbyD principle
- P's sound but don't add much value - PbyD principle

Issue with other powers - procedures

Square box

What privacy rights will be available

- So a period of selected change is at hand
 - in 2012 we regulate
 - as far as ICO itself
- want to ensure when handover in 2012 -
 - You will download new laws
 - and consider issues
 - of being about authoritative arbiter
 - of info rights - delivery of these
 - highly generally, relatively little
 - our concern should we aspire to
 - and help guide ~~we~~ 2013
 - aspiration and a clear policy
 - and work model of your
 - and work model of your

Apr - Jun 2012

2012 in a 12 month

work plan - Year - High level
High Priority IS10
High Priority IS10
IS10 will be on the

Data Protection:
Stronger enforcement
Greater encouragement

Jonathan Bamford
Head of Strategic Liaison



Sept 2010

A year
of big
changes
at the
ICO



ico.

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

ico.

Been involved in DP regulation 25 years
but last couple probably ~~seen~~^{been} the most
significant changes at substantive changes.

- This ~~couple~~ now makes up to why we have
DP laws in the place - how vulnerable
it can be in our institutions richness
- Train ~~people~~ ~~between~~ ~~within~~ ~~etc~~
Provide ICO with additional powers
not states to put on to other
- Train policies work up to us by
public sector and private of providers
in standards for here. And seen
get into government - transparency
and who putting citizen in control
into it works for agency.
- Also new new Commissioner
meet his job own the ICO
for for the challenges of how
- Want to give insight into ICO changes
how was effect you
- Imagine you are Chair of committee on
new powers
- New challenges around local new
DP framework

- Significant reorganisation
of our business units
Policy and Operations
- All focused on delivery
Mission. New business units
focused on articulated GP-Audit
- Information - MP
- Policy United DP/foi service -

Strategic Liaison Role

- Maintain and build key relationships and on key issues
- Support and advise key stakeholders
- Promote ICO information rights objectives
- Anticipate change
- Reduce risks

ico.

Member SL key roles

- Maintaining a difference with various individuals and on the issues that matter.

own to gain wider

learn from ICO issues, which

turn into intelligence

Strategic Liaison Structure

- Government and Society Group
- Public Service Group
- Public Security Group
- Business and Industry Group
- International Team

ico.

Break down into smaller groups

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.

- Changes, Penalties hit the risk

What do... - (ICO going away)
Shows negligence at highest - need to follow
strict process but value public

Serious breaches - strong penalties

MP Code factors like into
account.

Amount of Penalty
• Nature of contravention
• Effect of contravention
• Behaviour of Data Controller
• Impact on Data Controller
• Other Considerations
ico.

Significant breach. Look at who affected and how

Does it cause substantial damage or distress

Deliberate or failed to take reasonable steps

Of the penalty

Important part of principle
rel. to exec DC and others

- What does spouse

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.

Area where criticism going to DPA - consented with

partial retraction as some
Ass. Notice

- At Mo Comp. Dept. of
Offices - esp focus on
with implementation of existing DPA
Up to 110 small case - do
basis or risk.

Assessment Notices
• ICO will aim for co-operation
• Recommendations aimed at helping
• Developed capability - staff and audit practice
• Code of Practice
ico.

→ Not planned
→ If there
→ One web site

Ass. Notice - rule based appear
on hearing who
- Consistent with
- Common DC / Tech standards
- Business like
- DCI over audit rights
- New systems / process - new
- Stakeholders
- - input & involved
- no affect
- sensitive data
- delivery

9:50

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

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

ico.

So, in conclusion, good straightforward
of change. What is still more
changes at law.

- ~~more transparent ICO itself~~
- in the way ICO regulates
- ~~and giving ICO staff~~
- ~~and giving power~~

Treats a challenge to all

is to it is not an
~~information rights regime -~~
affordable, accessible and suitable
to those it's designed to protect

Information Commissioner's Office

Maureen H Falconer
Sr Guidance & Promotions Manager

Cloud Computing for the Public Sector



20th Sept 2010

The Law Makers

Data Protection Principles

Personal information must be:

- Processed fairly and lawfully
- Only obtained for specified lawful purposes
- Adequate, relevant and not excessive
- Accurate and, where necessary, kept up to date
- Not kept longer than necessary
- Processed in accordance with the rights of individuals
- Kept secure against unauthorised processing and accidental loss or destruction
- Not transferred outside the EEA unless adequate levels of protection

ico.

7th Data Protection Principle

DATA PROTECTION

The Data Protection Act 1998 requires that:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

ico.

Information Security

Security breaches
have SERIOUS implications.

Potential harm to individuals.

Damage to business reputation.

Breaches cost £££££££ ...



ico.

Security in the clouds

Data controller and data processor
relationship

Sector specific legislation and regulations

Adapt to changes in legislation and
regulations

Controlled access

Audit

ico.



Appropriate ...

Technical development at any given time to ensure a level of security appropriate to:

- the harm that might result from a breach, and
- the nature of the data to be protected;

Reliability of staff having access to the personal data;

Customised to specific circumstances;

ico.

...technical & organisational measures

Security management:

- Responsible senior person
- Sufficient resources
- Policies and procedures

Controlling access:

- Location controls
- Password protocols
- Secure disposal
- Remote access

Business continuity:

- Recovery plan
- Validation and backup
- Intrusion protection

Staff selection and training:

- Vetting and validation
- Job descriptions
- Continuous training
- Acceptable use

ico.

...technical & organisational measures

Breach management:

Audit trails;
Containment and
Recovery;
Assessing the risks;
Notification of breaches;
Evaluate and respond.

Data Processors:

Vetting and validation;
Ensure compliance;
Written contract;
Security standards;
Specific purposes;
Restricted practices.

ico.

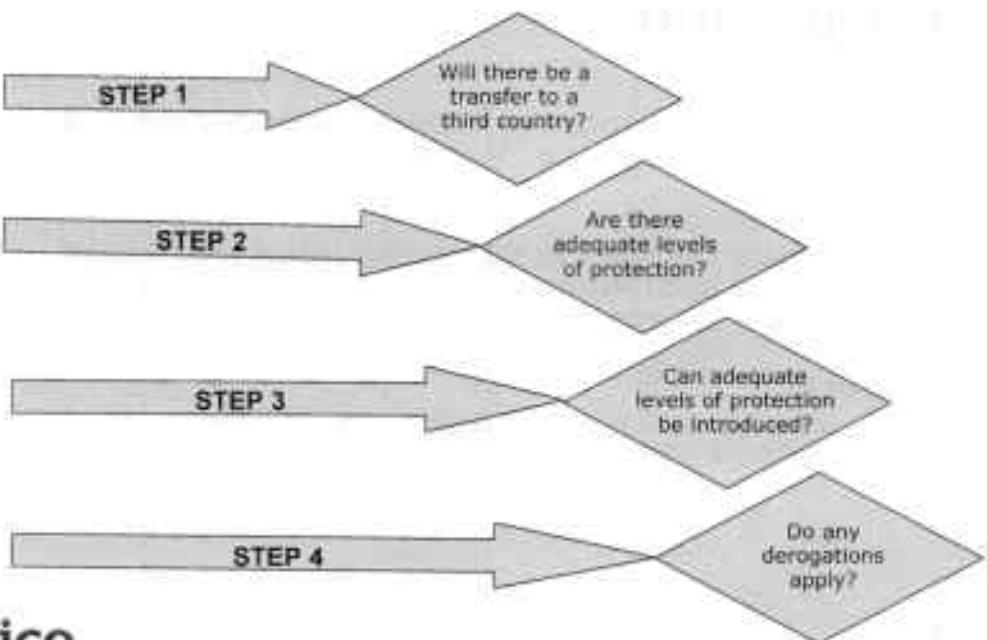
8th Data Protection Principle...

The Data Protection Act 1998 requires that:

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

ico.

Good practice approach...



ico.

Will there be a transfer to a third country?

Is it a Transfer?

- Must be a relocation to another country and not 'just passing through', i.e., in transit.

Is it a Third Country?

- Outside the EEA - all EU member states plus Iceland, Norway and Liechtenstein – anywhere else is considered to be a 'third country' according to the directive.

Is it Data?

- Includes data provided with a view to being computerised at the final destination.

ico.

Are there adequate levels of protection existing already???

European Commission findings of adequacy in the following:

Argentina

Canada

Guernsey

Safe Harbor Agreements in USA

Isle of Man

Switzerland

Jersey

Israel

Andorra

Faroe Islands

Assessing adequacy must consider:

the nature of data;

the country of origin;

the final destination;

the purposes and duration;

the relevant laws in force;

any international obligations;

codes of conduct or other rules;

existing security measures.

ico.

If not, can adequate levels be introduced?

Model Clauses:

European Commission approved model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set I & Set II controller-controller); data controllers in the EEA to data processors outside the EEA (controller-processors)

(2001/497/EC15; 2004/915/EC17; 2002/16/EC16).

Binding Corporate Rules:

Internal codes of conduct operating within a multinational organisation for the purposes of enabling transfer of data outside the EEA (but within the group) to be made on a basis which ensures adequate safeguards.

(must be approved by the Information Commissioner)

ico.

Do other derogations apply in spite of this?

Schedule 4 Conditions for transfer:

Consent of the data subject.

Necessary for the performance of, or entering into, a contract between the data subject and the data controller.

Necessary for the performance of, or entering into, a contract between the data controller and a third party entering into the contract at the request, or in the interests, of the data subject.

Necessary for reasons of substantial public interest.

Necessary in connection with legal proceedings, advice or rights.

Necessary to protect the vital interests of the data subject.

The transfer is of part of the personal data on a public register.

ico.

Information Commissioner's Office

**93-95 Hanover Street
Edinburgh
EH2 1DJ**

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



INFORMATION COMMISSIONER'S OFFICE

Sheila Logan
Operations and Policy Manager



20th Sept 2010

Information Security

Everyone's responsibility



ico.

Regulatory Action

7th Data Protection Principle

The Data Protection Act 1998 requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss destruction or damage.

ico.

Information Security

Security breaches
can have BIG implications.

Potential harm to individuals.

Damage to business reputation.



ico.

Security in the clouds

Data controller and data processor
Relationship

Sector specific legislation and regulations

Adapt to changes in legislation and
regulations

Controlled access

Audit

ico.



Physical Security

Controlled entry to buildings

Out of hours security

Visitor policy

Visible ID

Home working

ico.



Organisational Measures

Day to day responsibility for security.

Written procedures for staff to follow.

Excellent staff training.

Regular audits.

Monitoring change.

Investigating a security incident.

ico.

Real Benefits

Organisational efficiency;
Fewer complaints;
Less compensation;
Business reputation;
Customer confidence;
Overall reduction in **costs.**

ico.

Some things are not meant to be shared

Don't share:

Your password

Your remote access pass

Your computer privileges

Your identity

ico.



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

[ico.](http://www.ico.gov.uk)

Data Protection Workshop: Dispelling the myths of data protection and sharing data safely.

Maureen H Falconer
Sr Guidance & Promotions Manager

Citizens Advice Scotland Conference
September 2010



1st & 2nd Sept 2010



The (UK) Information Commissioner's Office...

- Regulatory Authority
 - DPA, PECR; FoI; EIR
- Regional Offices
 - Cardiff, Belfast, Edinburgh
 - Enquiries
 - Stakeholder engagement
 - Scottish input

ico.

Regulatory Authority

DPA; PECR; FoI; EIR

Role of the Regional Offices

- Established in response to devolution in Cardiff, Belfast and Edinburgh
- Enquiries helpline; general DP enquiries; referrals to Wilmslow
- Promotion of the ICO; regulator for the Data Protection Act & Freedom of Information Act in reserved issues
- Policy development; responding to consultations; feeding into the policy forum

Data Protection or Freedom of Information...

DPA

- Applies to personal information only
- Covers all sectors
- Gives individuals rights over their information
- Same Act north and south of the border

ICO

ico.

FOI

- Applies to general information only
- Public authorities only
- Gives everyone rights to general information
- Different Act north and south of the border

OSIC

DPA - PERSONAL DATA ONLY - If it's not personal data, then the Act does not apply.

FoI - GENERAL INFO' – NOT personal data

DPA - ALL SECTORS – Public, private & Voluntary.

FoI - PUBLIC AUTHORITIES ONLY – NOT private schools!

DPA - INDIVIDUALS – Right to own data only for individuals not organisations.

FoI - ANYONE – Application blind

DPA - SAME ACT – UK-wide legislation.

FoI - SEPARATE ACTS – reserved matter in Scotland

It applies everywhere...

BBC NEWS

You are in: **Education**
Front Page | World | UK | BBC Politics | Business | Sci/Tech | Health | **Education** | Hot Topics | UK Systems | League Tables | Festivals | Entertainment | Talking Point | In Depth | AudioVideo

Friday, 15 December, 2000, 16:27 GMT

Row over filming school shows



Michael Payne filmed sons Ben and Daniel after
A council has revised its ban on parents filming
their children in school plays, following an
outcry over the decision.

Search BBC News Online **GO**

Advanced search options

• [Recently commented](#) ↑
• [Recent news / editor's picks](#)

• [BBC RADIO NEWS](#)
• [BBC ONE TV NEWS](#)
• [WORLD NEWS SUMMARY](#)
• [BBC NEWS 24 BULLETIN](#)
• [PROGRAMME'S GUIDE](#)

See also:

- ▶ [24 Oct 00 | UK: Warning as net predator sentenced](#)
- ▶ [06 Jul 00 | UK: Talking at cross purposes](#)
- ▶ [19 Feb 00 | Education: Children warned against net predators](#)

ico.

It applies to everything...

heraldscotland

Wednesday 18 September 2008 | The Herald | sundayherald

[Front page](#) [News](#) [Sport](#) [Business](#) [Comment](#) [Blogs](#) [Arts & Ents](#)

[In Pictures](#) [Video & Audio](#) [Weather](#) [Crosswords & Sudoku](#) [News Feeds](#) [Risbs & Twitter](#)

BREAKING NEWS: [New drug](#)

Wait for it

KEN SMITH

Published on 30 Nov 2009

0 comments

As you might

An Edinburgh chap who provided a home for a friend's cat was bemused when he called the friend's vet for the cat's medical history, only to be told that under the Data Protection Act they couldn't pass on to him the cat's medical records.

His wife tried to calm him down by suggesting "it's perfectly reasonable - the cat may have had a medical procedure that it didn't want anyone to know about."

ico.

It defies common sense...

Telegraph.co.uk

[Home](#) [News](#) [Sport](#) [Finance](#) [Lifestyle](#) [Comment](#) [Travel](#) [Culture](#) [Technology](#)

[UK](#) [World](#) [UK Politics](#) [Celebrities](#) [Obituaries](#) [World](#) [Earth](#) [Science](#) [Health News](#) [Education](#)

[Royal Family](#) [Religion](#) [Read and Ball](#) [Defence](#) [Law and order](#) [Scotland](#)

[HOME](#) > [NEWS](#) > [UK NEWS](#)

Marks & Spencer demand 7-year-old boy's permission to deal with mother's complaint

A mother who complained to shop staff that her seven-year-old son's Superman playsuit was faulty was told data protection laws meant they could only deal with him

ico.

It defies logic...

Telegraph.co.uk

[Home](#) **News** [Sport](#) [Finance](#) [Lifestyle](#) [Comment](#) [Travel](#) [Culture](#) [Technology](#)

[UK](#) [World](#) [UK Politics](#) [Celebrities](#) [Obituaries](#) [Weird](#) [Earth](#) [Science](#) [Health News](#) [Education](#)

Royal Family Religion Road and Rail Defence Law and order Scotland

[HOME](#) > [NEWS](#) > [UK NEWS](#)

Royal Mail worker 'demands baby's signature'

A pensioner has complained that a postal worker refused to hand over a parcel to him unless his nine-day-old baby granddaughter signed for it

ico.

It's about Personal Data...

➤ Definitions:

- *Personal data* relate to a living individual who can be identified from those data and/or other information and includes opinions and intentions
- *Sensitive personal data* relate to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life, criminal activity

➤ Application:

- Files; Rights & Obligations; Conditions; Principles; Offences

ico.

DEFINITIONS

• **Personal Data** – relates to a **living** individual from which they can be **identified** or from which they can be identified with additional information to which the data controller has in or will come into his possession.

• **Sensitive Personal Data** – identifies specific aspects which are considered worthy of extra consideration before processing

APPLICATION

• **Files** - Applies to both electronic and manual files

• **Rights** - Provides rights to data subjects:

• **Obligations** – Sets out obligations for data controllers:

• **Conditions** – Sets out conditions for processing in Schedule 2 & 3

• **Principles** - Establishes 8 DP Principles as standards for processing personal data

• **Offences** – Creates specific criminal offences

It's about Files...

- Manual
 - Relevant filing system
 - Category (e) data (public authorities)

- Electronic
 - Data
 - Texts
 - Images
 - Recordings



ico.

RELEVANT FILING SYSTEM:

Temp-test; easily accessible by reference. Durant (2003): Biographical and Focussed, time/effort not considered.

CATEGORY e :

Four categories: **(a)** automated **(b)** intended to be automated **(c)** relevant filing system **(d)** accessible record (education, health, social work, housing)

(e) "Unstructured data" & "manual data" held by public authorities other than relevant filing system. PA must confirm whether it holds the data but not to comply with SAR unless a 'description' of the data is given or cost of complying is above appropriate limit £450 (£25/hr/person) (FoISA - £600 @ £15/hr/person).

Exempt from most of the Act except access and accuracy but Cat (e) personnel matters of PAs exempt from Principles and all PartII (rights).

It's about Rights & Obligations...

Individuals' Rights:

- Request a copy of personal data (S7)
- Stop unwarranted processing (S10)
- Stop direct marketing (S11)
- Know of automated decisions (S12)
- Personal data to be accurate (S14)
- Request an assessment (S42)
- Compensation (S13)

ico.

Organisations' Obligations:

- Respond within 40 days (S7)
- Respond within 21 days (S10)
- Comply without exception (S11)
- Provide alternative process (S12)
- Correct and alert those to whom disclosed (S14)
- Notify with ICO & notify changes (S18&20)
- Comply with Information/Enforcement Notice (S40&43)

ACCESS – SAR – In writing; verify identity; £10 fee; any other information. DC responds promptly and within 40 days.

STOP PROCESSING – Must be *unwarranted* and *substantial* damage or distress. DC must respond within 21 days by complying wholly or in part and state reason why.

DIRECT MARKETING - Request that DC stops within reasonable period. DC must comply, no exceptions.

AUTOMATED DECISIONS – eg: credit rating; insurance – no decision based on solely automated means but if so, can request a review of decision by other means. DC must give notice of such decision making.

INACCURACIES – As to a matter of fact not opinion. Entitled to insert a note of disagreement.

ASSESSMENT – Breach likely/unlikely and issue an enforcement notice to comply with the Act. DC must comply.

COMPENSATION – Only awarded by the court and must be quantifiable damage before distress can be claimed.

It's about Justification...

• Personal Data:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public interest
- Legitimate interest of data controller

ico.

Sensitive Personal Data:

- Explicit consent
- Employment law
- Vital interests
- Not-for-profit TU/religious/political/philosophical groups
- Already in public domain
- Legal proceedings/advice
- Public functions
- Medical purposes
- Equal Opps Monitoring
- Substantial public interest (SI2000/417)

It's about Standards...

Personal information must be:

- Processed fairly and lawfully
- Obtained only for specified lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Kept for no longer than necessary
- Processed in accordance with the rights of data subject
- Kept secure against unauthorised processing and accidental loss or destruction
- Not transferred outside the EEA unless adequate levels of protection

ico.

Fair Processing: individual is:

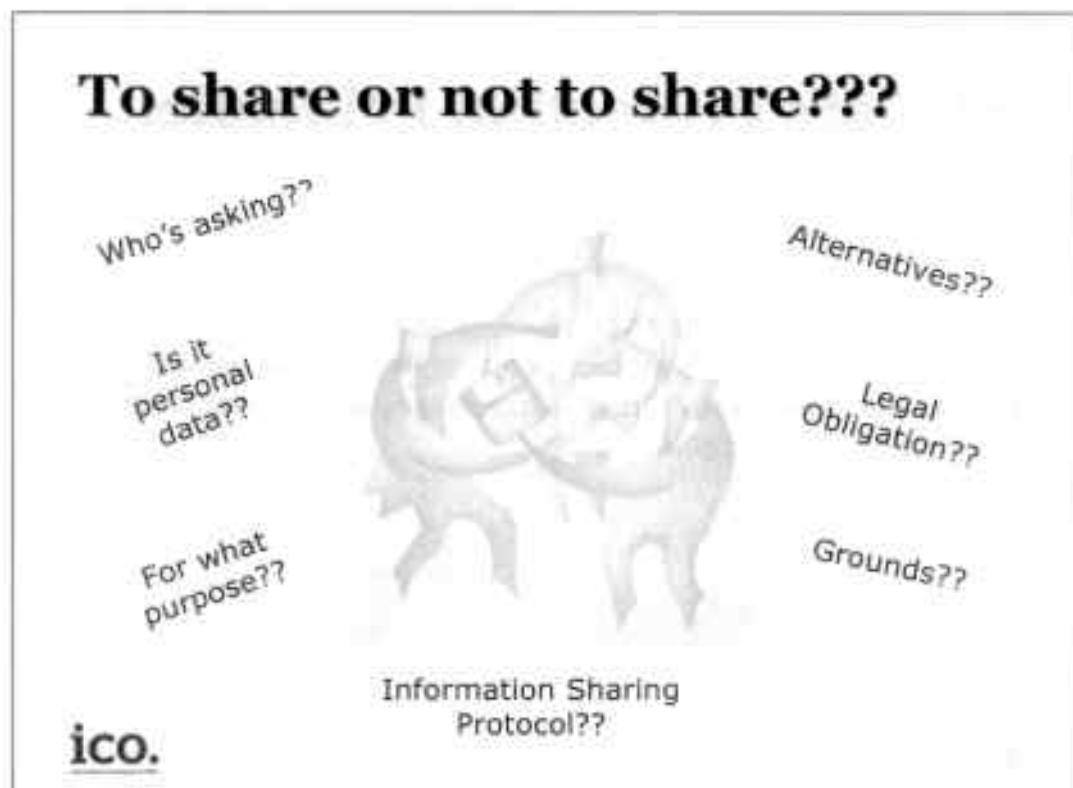
- informed of processing – **Who?**
- Informed of purposes – **Why?**
- Informed of disclosures – **How?**

Fair Processing Notice

Lawful Processing:

- Obtained legally
- Data controller notified with ICO
- Data subject's rights upheld
- Specified Purposes: those outlined in notification or FPN
- Do I need all this information? Do I have enough?
- Is it correct? Does it need amending?
- What is your retention policy?
- Is it compliant with the Principles?
- Is it safe?
- Can I send it there? EEA: all EU countries plus Switzerland, Iceland, Norway and Liechtenstein – **WEBSITES!!**

To share or not to share???



Who's asking? – Don't be afraid to say NO! Even if it's the police.

Is it personal? – If not, the Act does not apply!

Purpose? – Don't be afraid to ask why. It may be they can get it elsewhere but you are the easy option. Also, it must be in accordance with your stated purposes.

Alternatives? – Must it be personal data or can it be anonymised?

Legally obliged? – Do you have a choice or are you legally obliged to share?

Justification? – Can you rely on specific conditions to share?

Protocol? – If there is going to be regular sharing then draw up a protocol for all to agree on.

Producing your own protocol and using it will help you to establish good practice and to comply with the law. Following a good protocol should instill trust in your stakeholder and confidence in your staff.

7th Data Protection Principle...

The Data Protection Act 1998 requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss destruction or damage.

ico.

Technical Security...

Technical solutions
Training
Audit trails
Controlled access
Passwords



ico.

Technical – 'Appropriate' – best you can buy for the level of sensitivity

Training – New staff; new systems; regular reviews

Audit – Build in to system – IT; entry...

Access – Who sees what? Who needs to see what?

Passwords – No names or consecutive numbers, make them strong, don't keep them by the computer or on your pass!

Physical Security...

Controlled entry to buildings

Out of hours security

Visitor policy

Visible ID

Home working



ico.

Entry and exit points – should be controlled or monitored. Don't leave doors or windows open.

Out of Hours – clear desk policies, including secure cabinets for removable media.

Visitors – clear and enforced policy, escorted on and off premises.

Visible ID – If you've got it, flaunt it!! Visitors too!! Don't be afraid to challenge.

Home working – what policies and protocols are in place and are they adhered to, monitored and reviewed? How secure is the home computer?

Some things are not meant for sharing...



ico.

CASE STUDIES...

In your groups, discuss the case study and the various data protection/privacy issues which it raises and how they might be addressed.

Be prepared to share your findings with the other groups.

ico.

Information Commissioner's Office

**93-95 Hanover Street
Edinburgh
EH2 1DJ**

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



