Wednesday 20th October 2010

How the Data Protection Act 1998 applies to Cloud Computing

Kawser Hamid
Lead Policy Officer
Information Commissioner's Office

ICO can only talk about UK Law – but still relevant EU context

20-25min

Q at the end

Main topics

- The role and powers of the Information Commissioner's Office (ICO)
- An overview of the Data Protection Act 1998
- The ICO's view on how the Data Protection Act applies to Cloud Computing

ico.

The role and powers of the ICO

- Our role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

- Enforce and regulate
  - Freedom of Information Act 2000
  - Environmental Information Regulations 2004
  - Data Protection Act 1998
  - Privacy and Electronic Communications Regulations 2003

ico.

Provide information:

•First Contact department – telephone / written enq (used to be Customer service dept – aliens joke?)

•Produce guidance – see website

•Presentations

Promote good practice:

•Issue codes of practice e.g. CCTV, Employment, PIO – mention data sharing code and consultation

Adjudicate on complaints:

•Section 42 DPA – likely / unlikely

•Regulation 32 PECR – ask ICO to enforce powers under extended part 5 of DPA.

•Section 50 FOIA

•EIR – also section 50 of FOIA.

Maintain an official public register of Notified organisations – see later !

Our powers

- Information notices
- Enforcement notices
- Assessment notices
- Fine

ico.

Information notices – demand any info

- Section 43 DPA (offence – sec 47) and 51 FOIA – (contempt of court sec 54)

Enforcement notices – do what we decide

- Section 40 DPA (offence – sec 47) section 52 FOIA – (contempt of court sec 54)

Assessment notices

- section 41A of the DPA (amend by section 173 of Corners and Justice Act 2009) ICO may serve certain data controllers with a notice 'assessment notice')

1. imposing specific requirements on the DC determine whether the data controller has complied or is complying with the data protection principles
2. allows on site compulsory audit of certain bodies e.g. Govt dept or any PA designated by order.

- audits by permission of DC for all other bodies under section 51(7)

A notice served on government departments, any designated public authorities or any other organisations within designated categories for the purpose of enabling the Information Commissioner to determine whether the data controller has complied or is complying with the data protection principles i.e. to enable the carrying out of a compulsory audit (Section 41A Data Protection Act 1998).

Fine

- Section 55A of DPA (amend by section 144 criminal justice and immigration act 2008) ability to issue fine up to maximum of £500,000 for serious breach of principles (deliberate or reckless).

An overview of the Data Protection Act 1998

- Replaced the Data Protection Act 1984
- Framework for the use of personal data
- Technologically neutral
- Implements the 1995 EU Directive on Data Protection 95/46/EC

ico.

- Received Royal Assent on 16th July 1998
- Came into force March 1st 2000

NOT PRIVACY LAW ONLY!

EU Directive 95/46/EC
Required all EU DP to have basic minimum – required changes 1984 act
- ALL DC COVERED NOT JUST NOTIFIED
- APPLIES TO RFS AS WELL AS COMPUTER. NOT JUST COMPUTER

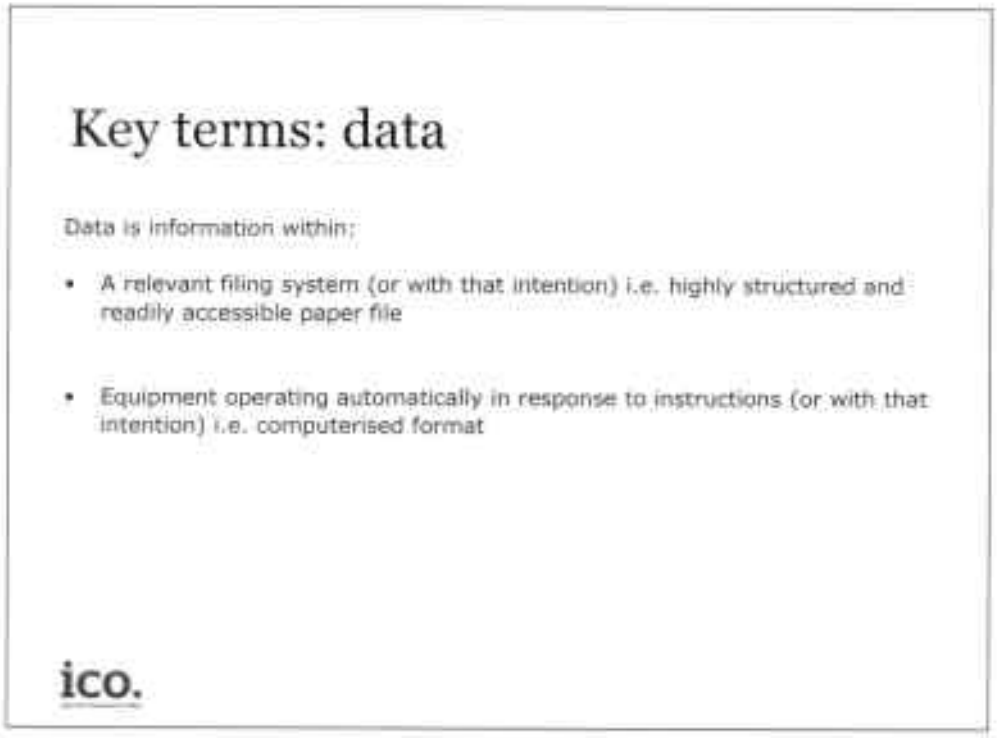
therefore 1998 act

Can't talk about rest of EU – but DPA basics will be in other EU countries DPA law

Directive under review – ICO SUBMISSION DEEDS TO TECHNOLOGICAL CHANGES
- Consultation July-Dec 2009 – 5 areas covered

1. Strengthening individuals rights
2. Data controller responsibility – harmonising approach / reduce administrative impact
3. The international transfer of information
4. How to incorporate criminal justice areas into new legislation – DIRECTIVE CURRENLTY NOT – EVEN THOUGH SOME ALREADY HAVE - HARMONISATION
5. Role of regulators – particular interest to us!

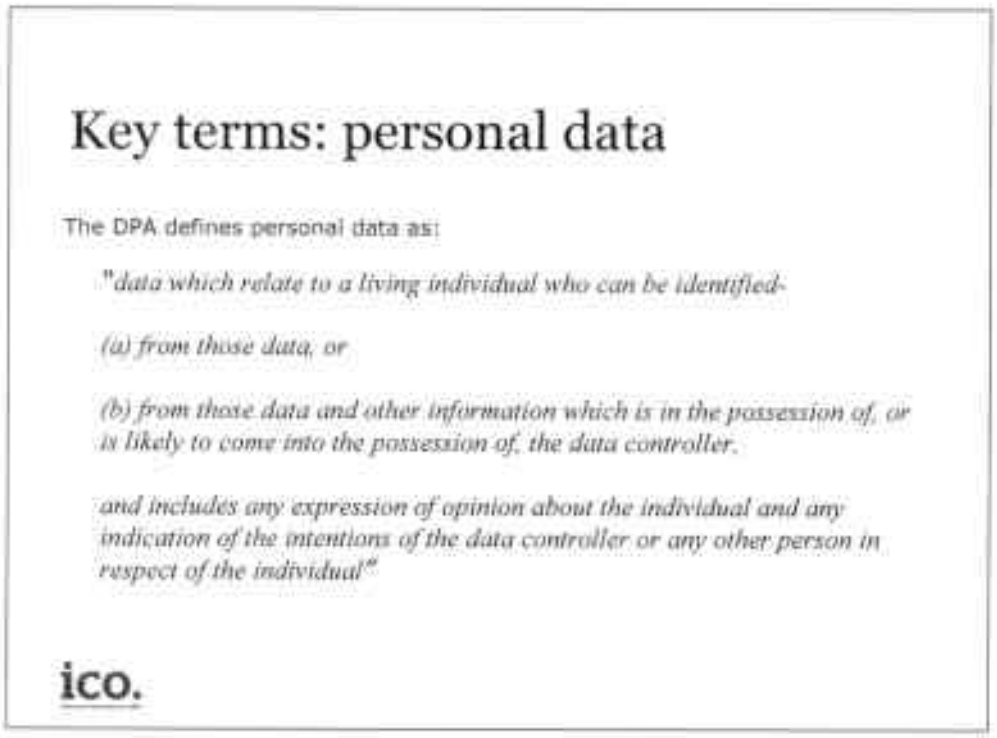
- Responses are currently being examined
- Should be communiqué end of this year giving some details on responses
- Legislation come into being mid 2011 – could be another directive or regulation



Say more about RFS?

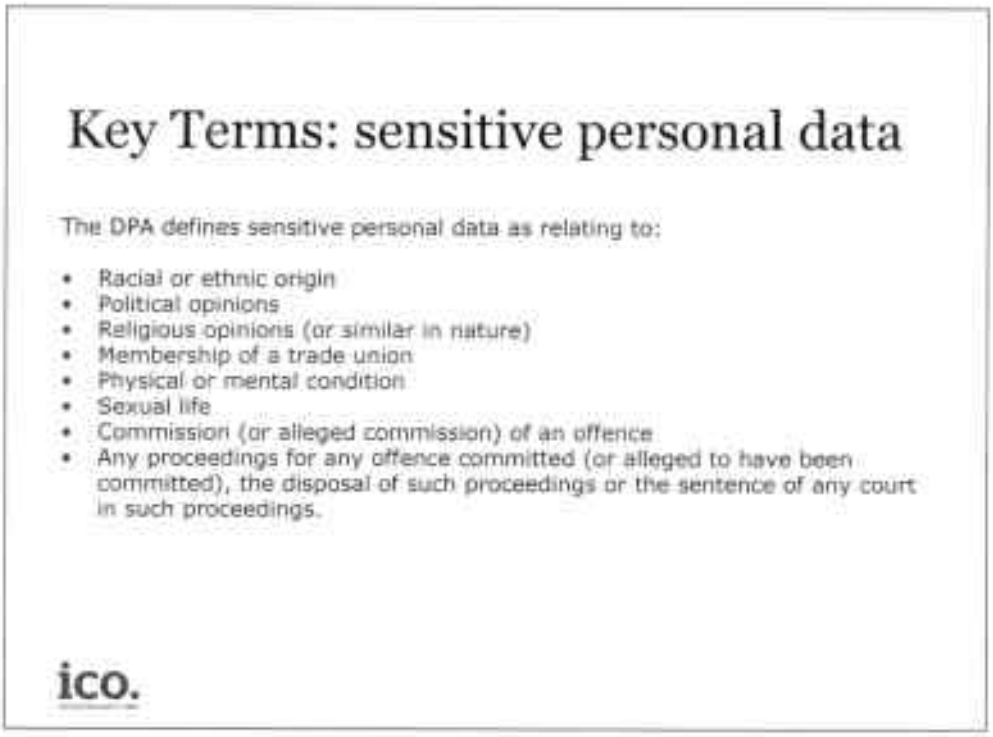
Accessible Record e.g. health record, educational record or housing record

Category e data – unstructured – FOIA – public authorities



Not dead people

Possession (or likely) to come in possession explain – e.g. disclosure example?



Section 2

Some fairly obvious why sensitive others not e.g. May find odd trade union listed but financial info not

Explain why trade unions on?

Other key terms

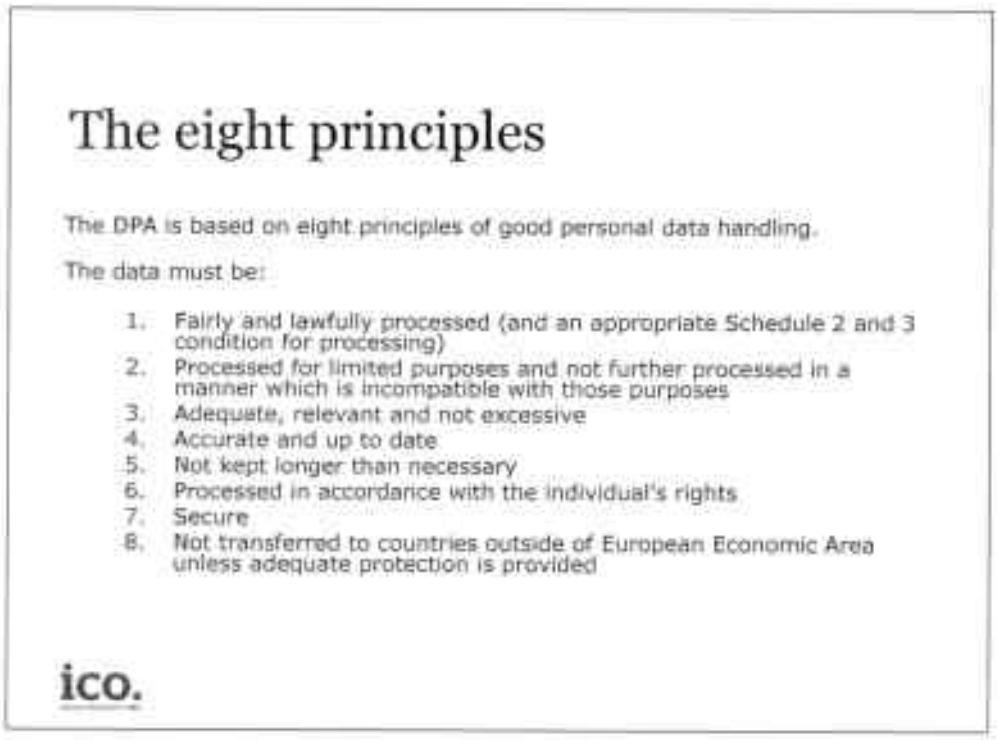
- Data Subject - an individual who is the subject of personal data
- Processing – virtually anything you can do to personal data e.g. hold, disclose, amend or delete
- Data Controller – a person who (either alone or jointly or in common with other persons) determines the purposes for and the manner in which any personal data are, or are to be, processed
- Data Processor - a person (other than an employee of the data controller) who processes the data on behalf of the data controller
- Disclosure – a data controller passing personal data to third parties

ico.

THIRD PARITES EXCLUDE

•DATA SUBJECT

•DATA PROCESSOR



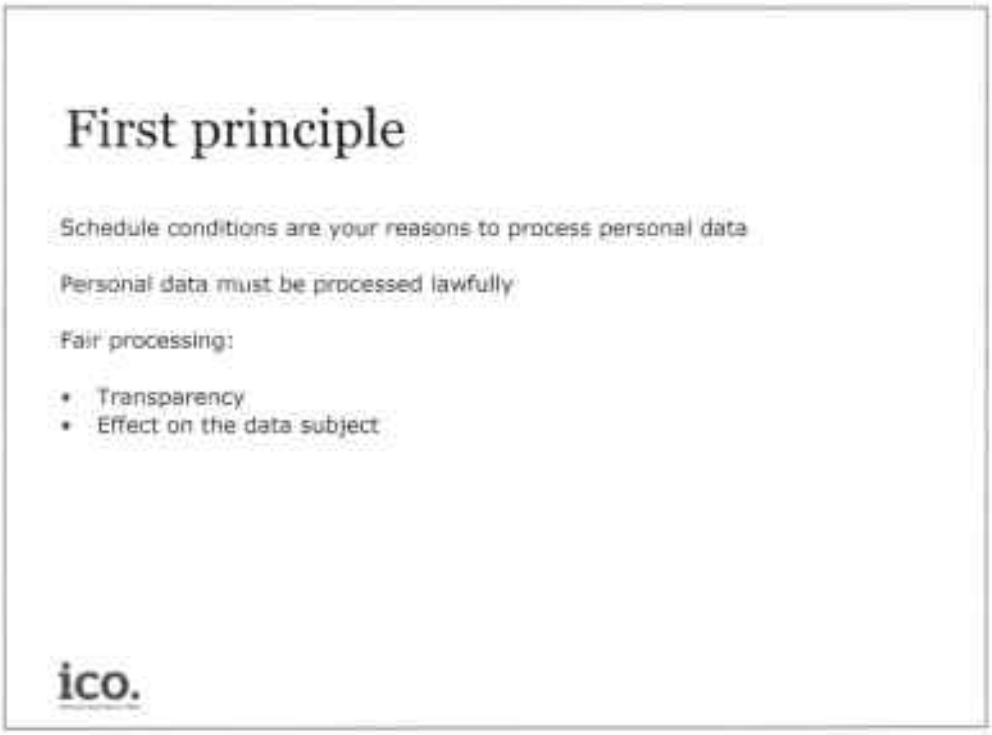
Most self explanatory – but require little more explaining PRINCIPLE 1 and some particularly relevant to CLOUD C PRINCIPLE 7 AND 8

First principle

The first principle states that:

> *"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met"*

ico.



DEAL WITHIN REVERSE ORDER – CONDITION – LAWFUL - FAIR

EXAMPLE OF SCH 2 CONDITION

•PROCESSING IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH DS IS A PARTY OR FOR TAKING STEPS AT THE REQUEST OF THE DS WITH A VIEW TO ENTERING INTO A CONTRACT

EXAMPLE OF SCH 3 CONDITION

•DS GIVEN EXPLICIT CONSENT

LAWFULNESS

•PUBLIC SECTOR BODY – NEED LEGAL POWER TO DO STUFF E.G. ICO LEGAL POWER COMES FROM DPA FOIA PECR EIR

•PRIVATE BODY – YOU JUST NEED TO MAKE SURE NOT BREAKING ANY LAW E.G. COMMOM LAW DUTY OF CONFIDENCE?

FAIRNESS

•IDENTITY OF DC / PURPOSES FOR WHICH GOING TO PROCESS PD / ANY OTHER INFO WHICH FAR TO TELL DS E.G. DISCLOSURES TO OTHER PARTIES (OR LEGITIMATE EXPECTATION OF DS)

•GENERAL CONCEPT OF FAIRNESS – WILL PROCESSING CAUSE ANY UNWARRANTED DAMAGE AND OR DISTRESS [INHERENTLY UNFAIR

Sixth principle

The sixth principle states that:

> *"Personal data shall be processed in accordance with the rights of data subjects under this Act."*

ico.

EXPLAIN IF OK FOR TIME

Sixth principle

Data subject rights

- Section 7 - Right of access to personal data (Subject Access Request)
- Section 10 - Right to prevent processing likely to cause substantial unwarranted damage and distress
- Section 11- Right to prevent direct marketing
- Section 12 - Rights in relation to automated decision taking
- Section 13 - Compensation for failure to comply with certain requirements
- Section 14 - Rectification, blocking, erasure and destruction of inaccurate personal data

ico.

SECTION 7
•IN WRITING
•£10 SOMETIMES £50 FOR MEDICAL RECORDS FEE
•PROOF OF IDENTITY
•ANY INFORMATION DC NEED TO HELP LOCATE PD
•INFO TO BE PROVIDED 40 DAYS – UNLESS EXEMPTION E.G. SECTION 29 – SAY MORE LATER

SECTION 10
•IN WRITING REQUEST STOP PROCESSING BECAUSE CAUSING SUBSTANTIAL UNWARRANTED DAMAGE AND DISTRESS TO DS OR OTHER
•DC RESPOND TO IN 21 DAYS IN WRITING EXPLAINING THAT IT WILL COMPLY OR EXPLAIN WHY IT WILL NOT
•DS CAN GO STRAIGHT TO COURT TO ENFORCE

SECTION 11
•IN WRITING ASK DC NOT USE PERSONAL DATA FOR DIRECT MARKETING PURPOSES
•ENFORCE THROUGH COURT

Section 12
•an individual can give written notice requiring you not to take any automated decisions using their personal data;
•even if they have not given notice, an individual should be informed when such a decision has been taken; and
•an individual can ask you to reconsider a decision taken by automated means.
•ENFORCE THROUGH COURTS

SECTION 13
•COURT AWARDS COMPENSATION

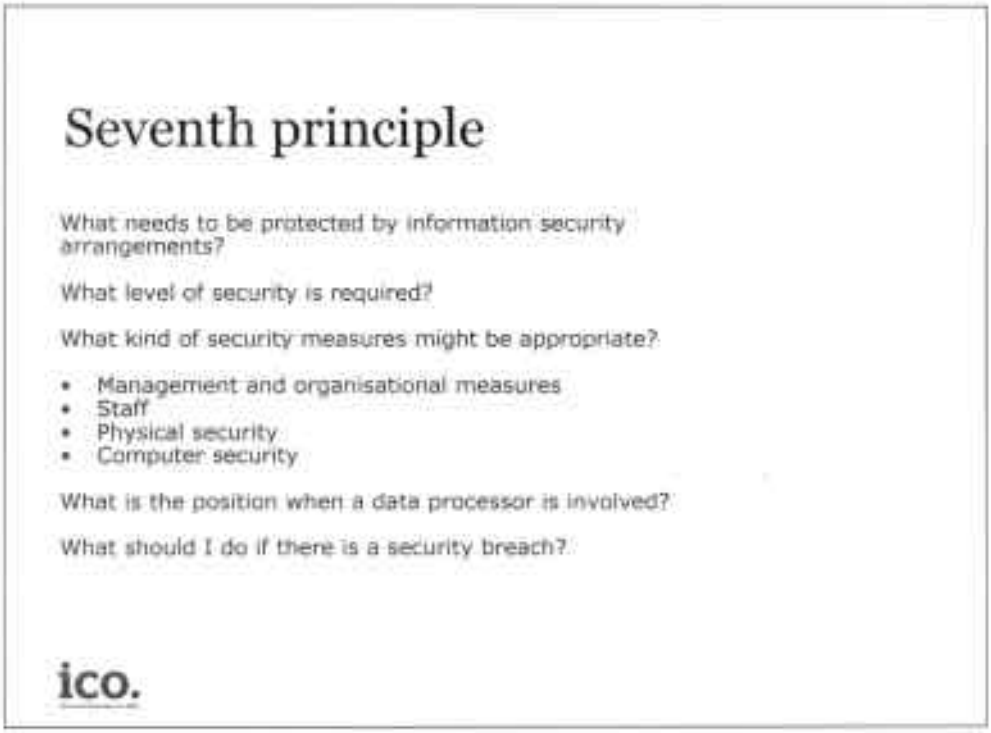
SECTION 14
•IF COURT SATISFIED INFO IN ACCURATE CAN ORDER RBED

Seventh principle

The seventh principle states 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.



•design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;

•be clear about who in your organisation is responsible for ensuring information security;

•make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and

•be ready to respond to any breach of security swiftly and effectively.

SECURITY BIG ISSUE – DATA LOSS HMRC

ENCRYPTION

PRIVACY BY DESIGN – PETS –

•DATA MINMISATION

•PSEUDONYMS

•BLIND SIGNATURES

•TRUSTED THIRD PARTIES

•ENCRYPTION

PRIVACY IMPACT ASSESSMENTS

Eighth principle

The eighth principle states 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 for the rights and freedoms of data subjects in relation to the processing of personal data"*

ico.

A transfer involves sending personal data to someone in another country – EVEN IT ITS WITHIN THE SAME COMPANY / DATA CONTROLLER

A transfer is not the same as the transit of information though a country. The eighth principle will only apply if the information moves to a country, rather than simply passing through it on route to its destination.

EEA - EU plus Norway, Licten and Iceland

DECIDING "ADEQUATE" factors you should take into account to make this decision. These relate to:

- the nature of the personal data being transferred;
- how the data will be used and for how long; and
- The laws and practices of the country you are transferring it to

ASSESSING laws and practices of the country you are transferring it to:

- the extent to which the country has adopted data protection standards in its law;
- whether there is a way to make sure the standards are achieved in practice; and
- whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

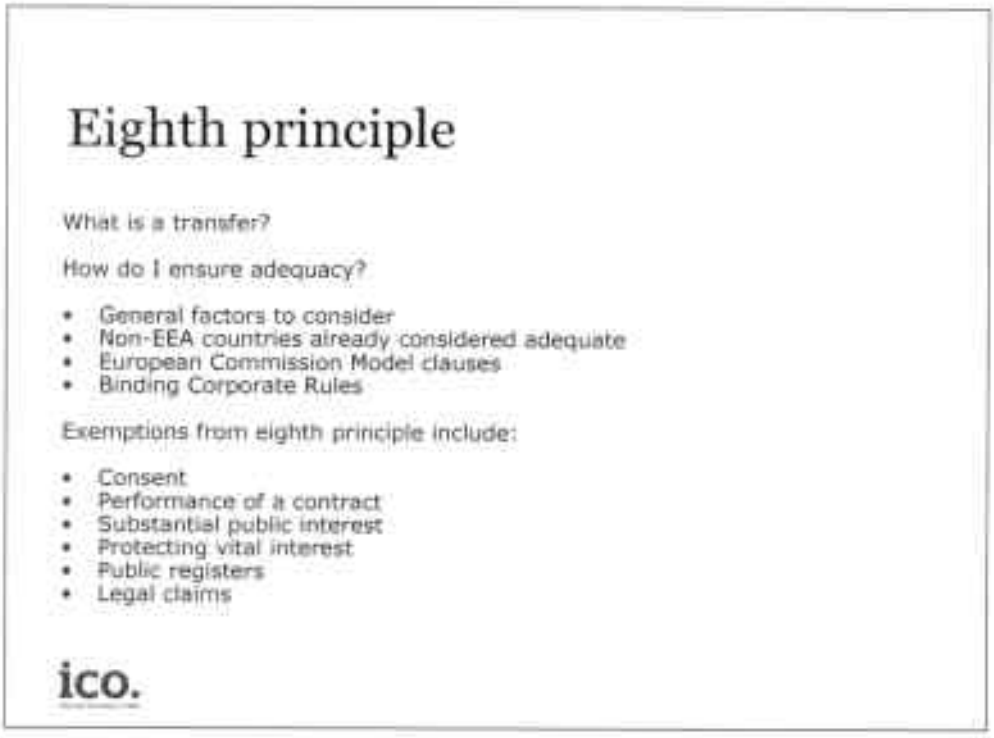
Countries considered adequate include - Argentina, Switzerland, Canada, Guernsey and Isle of Man

Safe Harbour Agreement - USA - Personal information can also be transferred to companies in the US that have signed up to the 'Safe Harbor' agreement. These companies have agreed to abide by a set of rules similar to those found in our own data protection law

EC model clauses

- The European Commission has approved three sets of standard contractual clauses (known as model clauses) as providing an adequate level of protection. If you use these model clauses in their entirety in your contract, you will not have to make your own assessment of adequacy.

- Two of the sets of model clauses relate to transferring personal data from one company to another company, which will then use it for its own purposes. In this case you can choose either set of clauses, depending on which suits your



DECIDING "ADEQUATE" factors you should take into account to make this decision. These relate to:

•the nature of the personal data being transferred;
•how the data will be used and for how long; and
•The laws and practices of the country you are transferring it to.

ASSESSING laws and practices of the country you are transferring it to:

•the extent to which the country has adopted data protection standards in its law;
•whether there is a way to make sure the standards are achieved in practice; and
•whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

Countries considered adequate include - Argentina, Switzerland, Canada, Guernsey and Isle of Man

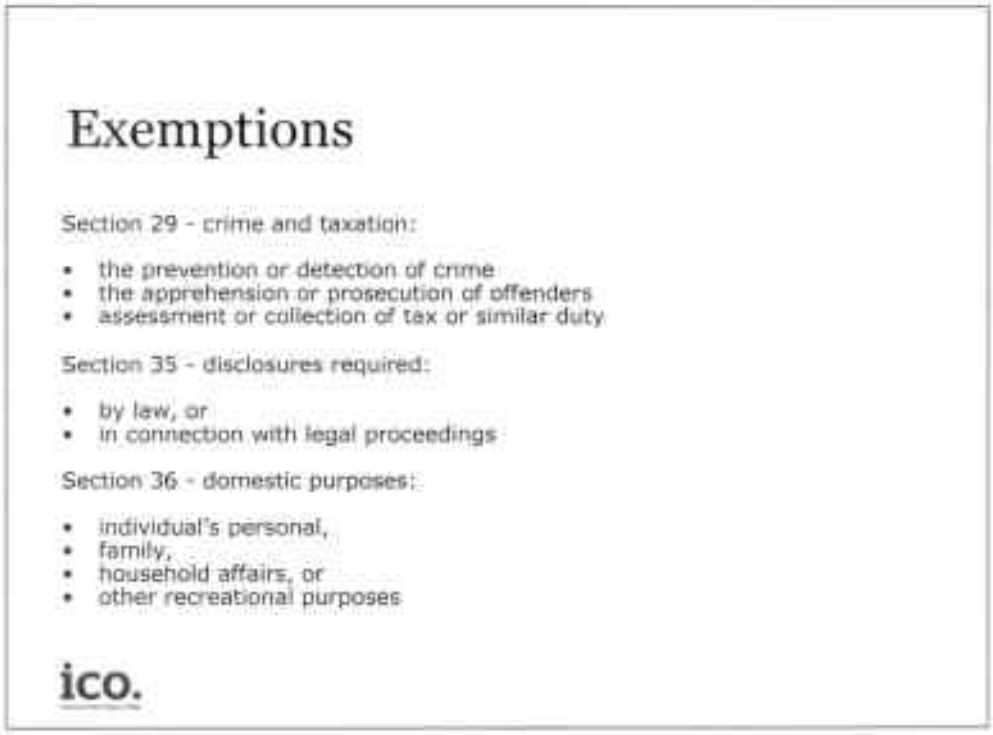
Safe Harbour Agreement - USA - Personal information can also be transferred to companies in the US that have signed up to the 'Safe Harbor' agreement. These companies have agreed to abide by a set of rules similar to those found in our own data protection law

EC model clauses

•The European Commission has approved three sets of standard contractual clauses (known as model clauses) as providing an adequate level of protection. If you use these model clauses in their entirety in your contract, you will not have to make your own assessment of adequacy.

•Two of the sets of model clauses relate to transferring personal data from one company to another company, which will then use it for its own purposes. In this case you can choose either set of clauses, depending on which suits your business arrangements better. The other set of model clauses is for transferring personal data to a processor acting under your instructions, such as a company that provides you with IT services or runs a call centre for you.

•The model clauses are attached as an annex to the European Commission decisions of adequacy, which approve their use. The Information Commissioner has authorised the use of model contracts for transfers from controller to controller and controller to



DETAIL IF GOT TIME

THERE ARE OTHERS MORE MAY BE PARTICULARLY RELEVANT TO PRIVATE SECTOR:

•Schedule 7(5) - management forecasts

•Schedule 7(6) – corporate finance

•Schedule 7(7) – negotiations

EXEMPT FROM SAR AND FAIR PROCESSING – IF LIKELY TO PREJUDICE

Notification

- The ICO maintains a public register of notified data controllers
- Transparency
- A data controller must notify if it is processing personal data in a computerised format
- Notification costs £500 per year for large organisations and £35 for everyone else
- Exemptions from notification

ico.

DETAIL IF GOT TIME

TRANSPARENCY - Data Subjects / Data Classes / Recipients

The two-tier structure is based on organisation size and turnover:

•A new notification fee of £500 applies to data controllers with either a turnover of £25.9M and 250 or more members of staff , or

•if they are a public authority with 250 or more members of staff.

All other data controllers remain in the lower-tier category, paying £35 per annum unless they are exempt.

But there are exemptions from notification if the processing is for:

Only domestic / recreational purposes

Only the following business purposes:

- Staff Administration
- Accounts and Records
- Advertising, Marketing and Public Relations (for your own purposes)

not-for-profit organisation – IF THEY
•HAVE REGULAR CONTACT WITH DS E.G. NOT CAB
•DO NOT SELL ON DATABASES
•NO CCTV

Only for the maintenance of a public register

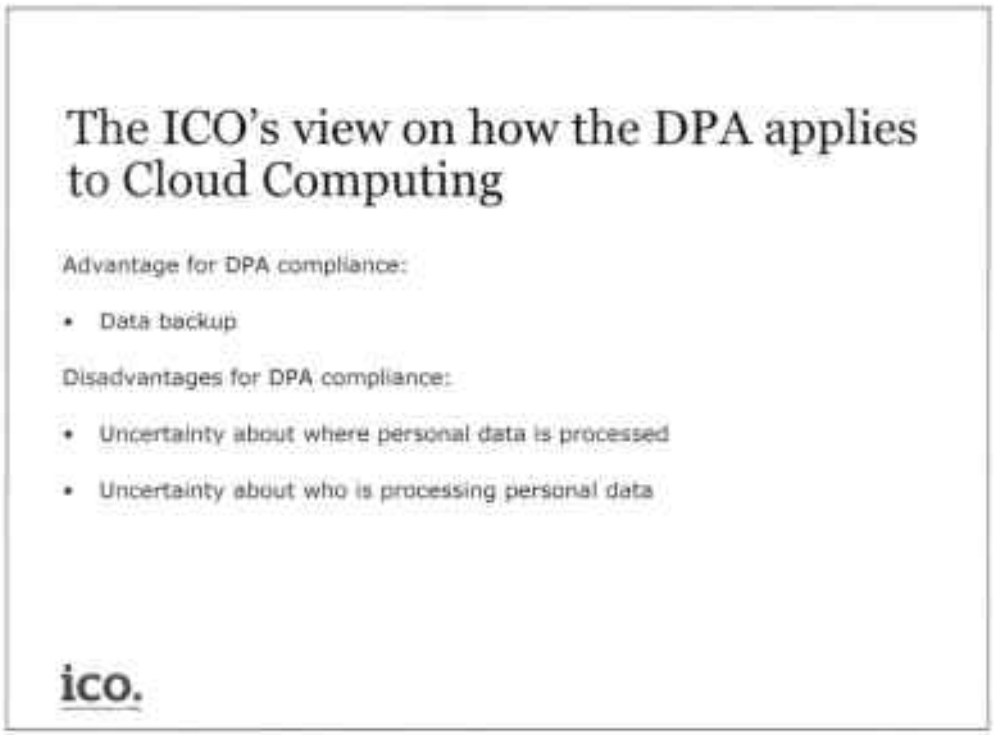
•OFFENCES
•Section 21(1): processing without notification (if you are required to notify)
•Section 21(2): failure to keep notification up to date

Offences

- Section 21(1): processing without notification (if you are required to notify)
- Section 21(2): failure to keep notification up to date
- Section 47(1): failure to comply with an information / enforcement notice
- Section 55: obtaining and / or disclosure of personal data without the consent of the data controller
- Section 77 of the FOIA: altering / deleting records with intention to prevent disclosure under section 7 of the DPA

ico.

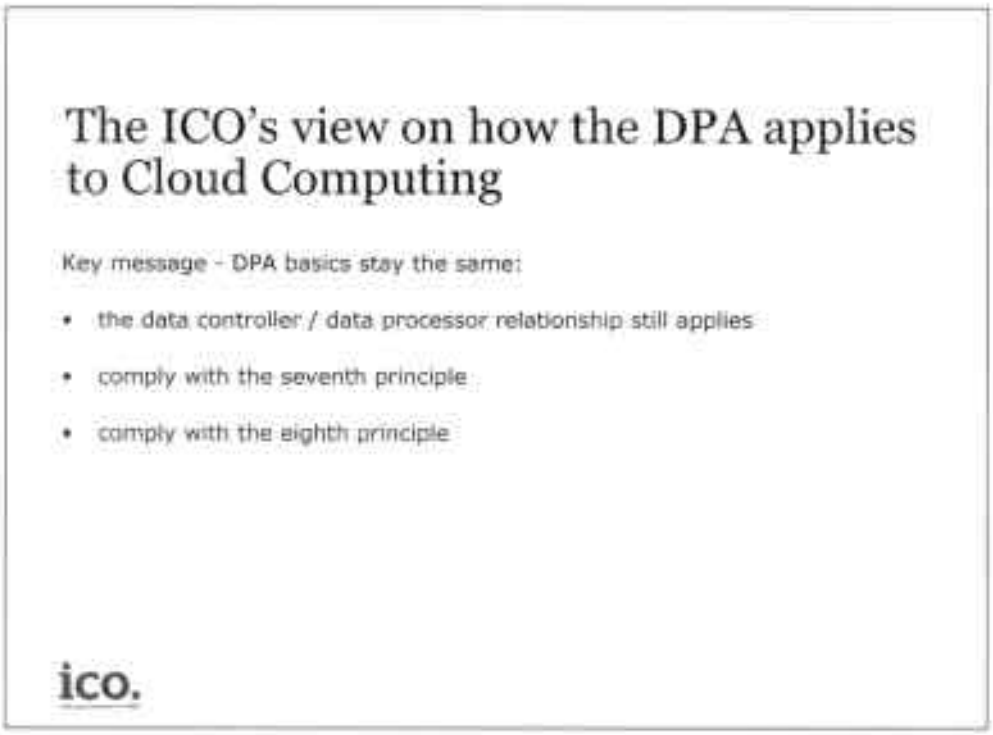
DETAIL IF GOT TIME



•CC NEW AND DIFFERENT TYPE OF COMPUTING APPROACH

•ADVANTAGE - ON SITE MAINFRAME FIRE EXAMPLE

•DISADVANTAGES - COMPLEX CHAINS OF CONTRACTORS AND SUBCONTRACTORS



•Maybe harder to implement DPA basic THAN COVENTIONAL ARRANGEMENTS

•CC PURCHASER – DC, CC PROVIDER DP

•SECURITY – CONTRACT / ENCRYPTION

CAN I ANSWER THESE Q'S – MORE EXTENSIVE LIST IN PIO

Contact us:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Helpline: 0303 123 1113
Fax: 01625 524510
E-mail: mail@ico.gsi.gov.uk
Website: www.ico.gov.uk

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

ON WEBISTE YOU CAN FIND GUIDANCE, PARTICULARLY:

•PIO CODE

•PRIVACY BY DESIGN

How the Data Protection Act 1998 applies to Cloud Computing

Kawser Hamid
Lead Policy Officer
Information Commissioner's Office

20th October 2010

The role and powers of the ICO

- Oversee and enforce:
  - Freedom of Information Act 2000
  - Environmental Information Regulations 2004
  - Data Protection Act 1998
  - Privacy and Electronic Communications Regulations 2003

ico.

Our role

- Provide information to individuals and organisations
- Promote good practice
- Adjudicate on complaints
- Maintain an official public register of notified organisations

ico.

Provide information:

•First Contact department – telephone / written enq

•Produce guidance – see website

•Presentations

Promote good practice:

•Issue codes of practice e.g. CCTV, Employment, PIO – mention data sharing code

Adjudicate on complaints:

•Section 42 DPA – likely / unlikely

•Regulation 32 PECR – ask ICO to enforce powers under extended part 5 of DPA.

•Section 50 FOIA

•EIR – also section 50 of FOIA.

Maintain an official public register of Notified organisations – see later !

Our powers

- Information notices
- Enforcement notices
- Assessment notices
- Fine

ico.

Information notices – demand any info

- Section 43 DPA (offence – sec 47) and 51 FOIA – (contempt of court sec 54)

Enforcement notices – do what we decide

- Section 40 DPA (offence – sec 47) section 52 FOIA – (contempt of court sec 54)

Assessment notices

- section 41A – SERVE DC with 'assessment notice')

1. to determine whether DC has complied or is complying with the DP principles
2. allows on site compulsory audit of certain bodies e.g. Govt dept or any PA designated by order.

- audits by permission of DC for all other bodies under section 51(7)

Fine

- Section 55A of DPA ability to issue fine up to maximum of £500,000 for serious breach of principles (deliberate or reckless).

NOTICE CAN BE APPEALED TO INFORMATION TRIBUNAL

What is data protection?

- Information that identifies a living person
- Responsibilities for 'data controllers'
- Not just security
- Transparency
- Fairness
- Information standards
- Overseas transfer rules
- Rights for individuals

ico.

Definition in Act more complex - Personal data

Determines the purposes of and the manner in which...

Who you are, why you are processing, anything else...

Object/impact/different

Adequate/relevant/not excessive/accurate

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 for the rights and freedoms of data subjects in relation to the processing of personal data.

What is a transfer?

How do I ensure adequacy?

•General factors to consider
•Non-EEA countries already considered adequate
•European Commission Model clauses
•Binding Corporate Rules

Exemptions from eighth principle include:

•Consent
•Performance of a contract
•Substantial public interest
•Protecting vital interest
•Public registers
•Legal claims

Cloud computing and the DPA: does it change anything?

- We don't think so!
- Breaks down into 'classical' DP compliance issues:
  - Data controller responsibility
  - Transparency
  - Overseas transfer rules
  - Security

ico.

DC responsibility - cloud provider = data processor – contract

Transparency - COMPLEX CHAINS OF CONTRACTORS AND SUBCONTRACTORS

Overseas - as above – problems will arise deciding if such protections exist

Security – what assurances can cloud provider give?

ICO's key messages on Cloud Computing

DPA basics stay the same:

- The data controller / data processor relationship still applies.
- Have adequate security.
- Make sure overseas transfers have adequate protection for rights and freedoms of the data subject.

ico.

•Maybe harder to implement DPA basic THAN COVENTIONAL ARRANGEMENTS

•CC PURCHASER – DC, CC PROVIDER DP

•SECURITY – CONTRACT / ENCRYPTION?

Choosing a Cloud Computing service provider

We recommend the following questions:

- Can it guarantee the reliability and training of its staff, wherever they are based? Do they have any form of professional accreditation?
- What capacity does it have for recovering from a serious technological or procedural failure?
- What are its arrangements and record regarding complaints and redress – does it offer compensation for the loss or corruption of data entrusted to it?
- What assurances can it give that data protection standards will be maintained, even if the data is stored in a country with weak, or no, data protection law, or where governmental data interception powers are strong and lacking safeguards?

ico.

CAN I ANSWER THESE Q'S –

Personal information online

ico.

MORE EXTENSIVE LIST IN PIO – will be revised to say more about cloud and revised PECR

ICO looking to work on issue of cloud service providers' T&C's

Mention new data sharing code

Contact us:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Helpline: 0303 123 1113
Fax: 01625 524510
E-mail: casework@ico.gsi.gov.uk
Website: www.ico.gov.uk

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