Securing Information Rights in the Cloud

Simon Rice
Principal Policy Adviser (Technology)
14 October 2011

ico.
Information Commissioner's Office

Overview

- The Information Commissioner's Office
- Cloud Computing: A definition
- DPA98 vs. The Cloud
  - The Risks?
  - The Solutions?
- Eliminating the risks
  - Privacy by Design

ico.
Information Commissioner's Office

Who is the ICO?

- The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals
- Enforces and regulate:
  - Data Protection Act
  - Freedom of Information Act
  - Environmental Information Regulations
  - Privacy and Electronic Communications Regulations

ico.
Information Commissioner's Office

How do we do this?

- Provide information to individuals and organisations
- Adjudicate on complaints
- Promote good practice
- Enforcement
  - Civil Monetary Penalties
- Audit

ico.
Information Commissioner's Office

Why is this relevant today?

- DPA98 regulates all *personal data processed by automatic means*
- Huge increase in online security breaches
- SPAM texts
- Illegal trading in personal data
- New technologies
  - Smart phones / Geo-location
  - Biometrics in private industry
  - Cloud computing

ico.
Information Commissioner's Office

Back to “the cloud”

ico.
Information Commissioner's Office

Cloud computing: What is it?

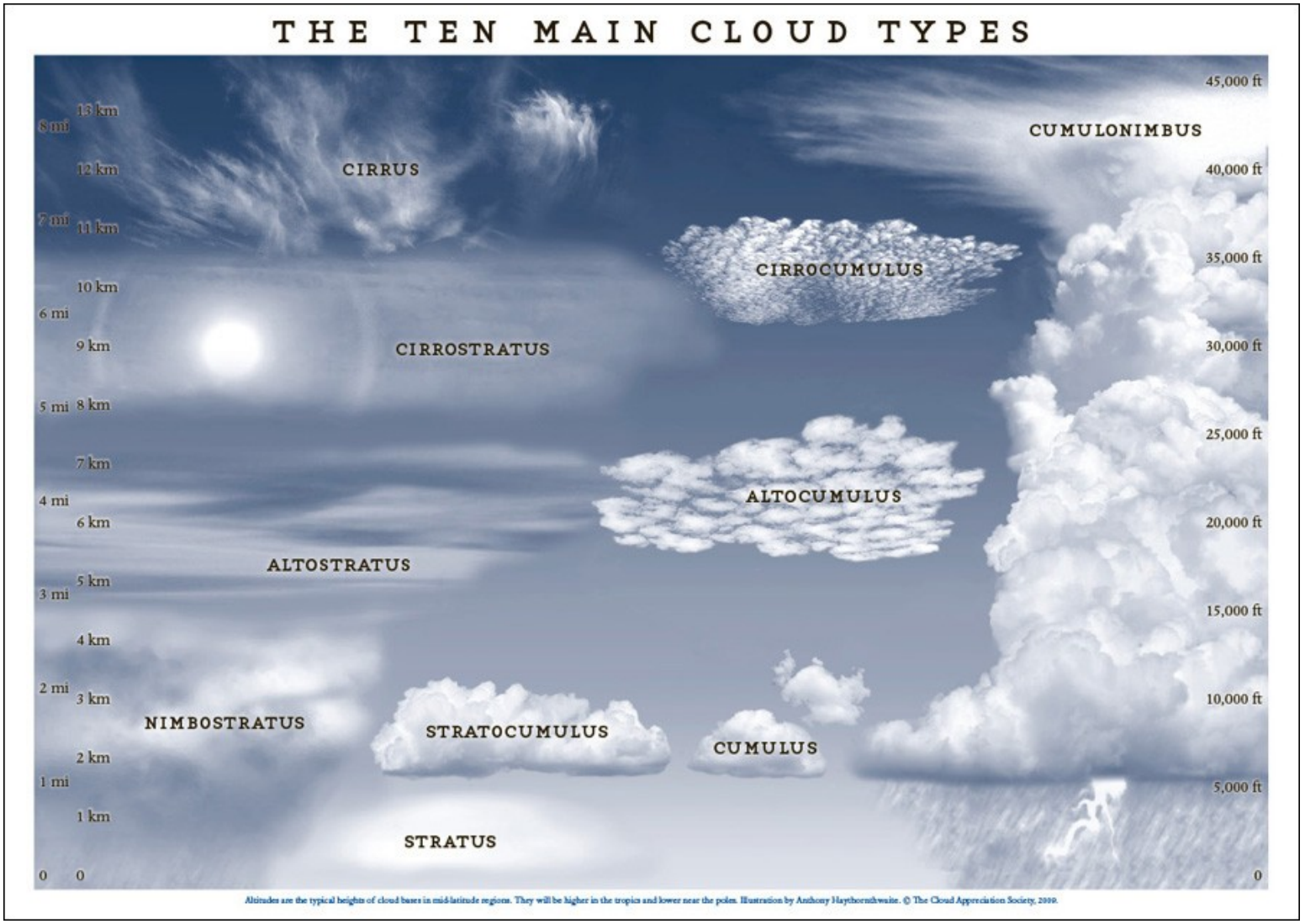
Who has knowingly used a cloud computing resource?

What about:

- Web-based email: *Hotmail, Gmail*
- Online Software: *Microsoft 365*
- Social media: *Facebook, Twitter, Flickr*
- Mobile devices: *iOS, Android*
- Backup/Storage: *AWS, Dropbox, BT Vault*
- Hosting: *Rackspace, Google Sites*

ico.
Information Commissioner's Office

Not all clouds look the same!



ico.
Information Commissioner's Office

Cloud computing: A definition

"Access to computational resources on demand via a network"

Computational resources

*"Access to **computational resources** on demand via a network"*

- Storage
- Processor
- Memory
- Files
- Software

IaaS

SaaS

On demand

*"Access to computational resources **on demand** via a network"*

- "How much you want"
- Often on a pay-per-use basis
- Utility computing

Via a network

*"Access to computational resources on demand **via a network"***

- Implies some data transit
- Likely a transfer to a different network
- May be outside of your direct control (i.e. public cloud)

DPA98: Back to basics

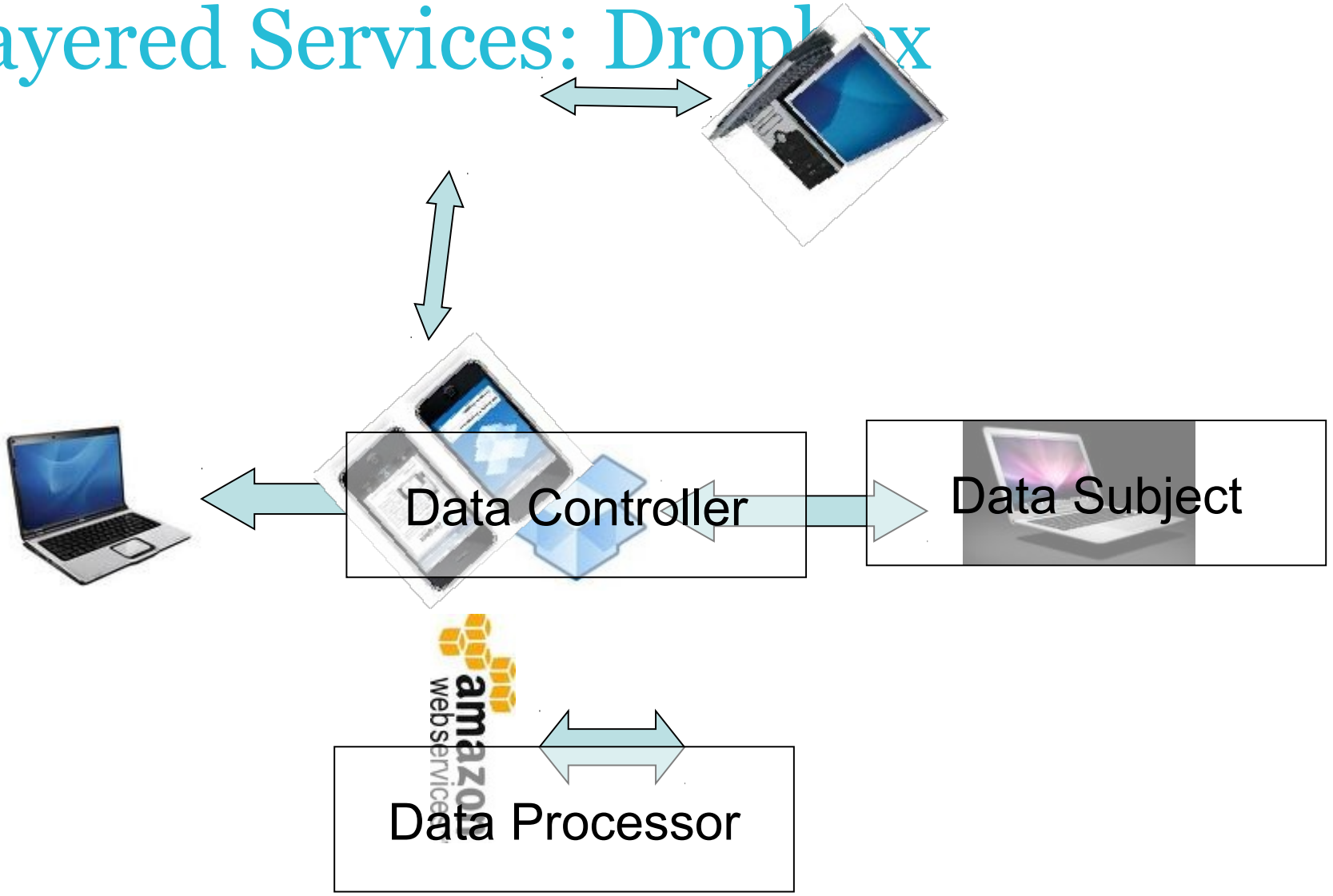
- Data Controller
  - A person who determines the purposes and the manner in which any personal data are, or are to be, processed
- Data Processor
  - A person who processes the data on behalf of the data controller
  - Processor acts solely on the instructions of the controller
- Liability lies with the controller
- Who is the data controller and the data processor?

Who determines the processing?

		Community	Public
IaaS P			
SaaS			

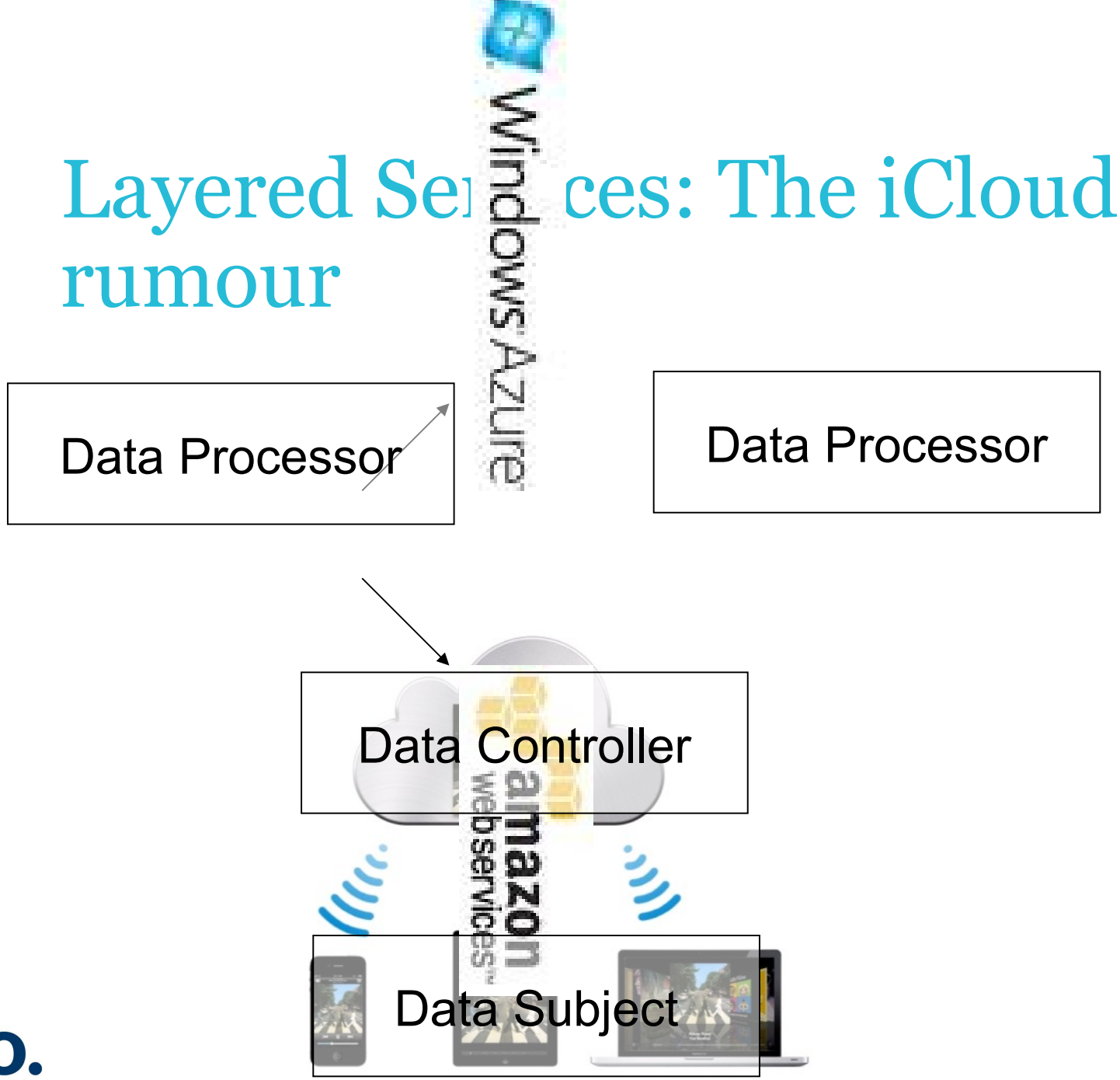
ico.
Information Commissioner's Office

Layered Services: Dropbox



ico.
Information Commissioner's Office

Layered Services: The iCloud rumour



ico.
Information Commissioner's Office

The corporate example

Data Processor

Data Controller

Data Subjects

What are the data protection issues?

- What is personal data?
- Who can see my personal data?
- Where is my personal data?

- Is there really anything new here?
  - Security
  - Outsourcing
  - Overseas transfer rules

ico.
Information Commissioner's Office

What are the data protection benefits?

- Potential to be more user-centric
  - Data subject can be in control
  - Improved subject access
  - Data subject can keep things up-to-date
- Greater transparency / Accountability
- Potential for increased security from a dedicated provider

What is personal data?

1. The personal data you place in the cloud
    - User profiles
    - User data
    - Customer data
2. Meta-data
    - Usage data you collect about users
    - Usage data your cloud provider collects about your users

ico.
Information Commissioner's Office

Who can see my data?

- Security (Principle 7)
  - Physical security
  - Encryption
    - in transit (to **and** within the cloud provider)
    - at rest
    - during processing*
  - Passwords & remote access
- Provider access
- Data disclosure
- Access by my neighbours*

Where is my personal data?

- Multiple copies in multiple locations
  - Where are the data centres?
  - Redundant copies
  - Back-ups
- Sharding
- Shared resources
  - Deletion
  - Retention
- Layered services
  - Is your SaaS provider using a different IaaS provider?
- Overseas Transfers (Principle 8)

ico.
Information Commissioner's Office

Other risks?

- Loss of governance (who has access?)
- Lock-in (can you transfer to somewhere else?)
- Isolation failure (eggs in one basket?)
- Data segregation (who's data is next to yours?)
- Regulatory compliance (can you really transfer the risk?)
- Data location (where is your data?)
- Data recovery (can you get it back?)

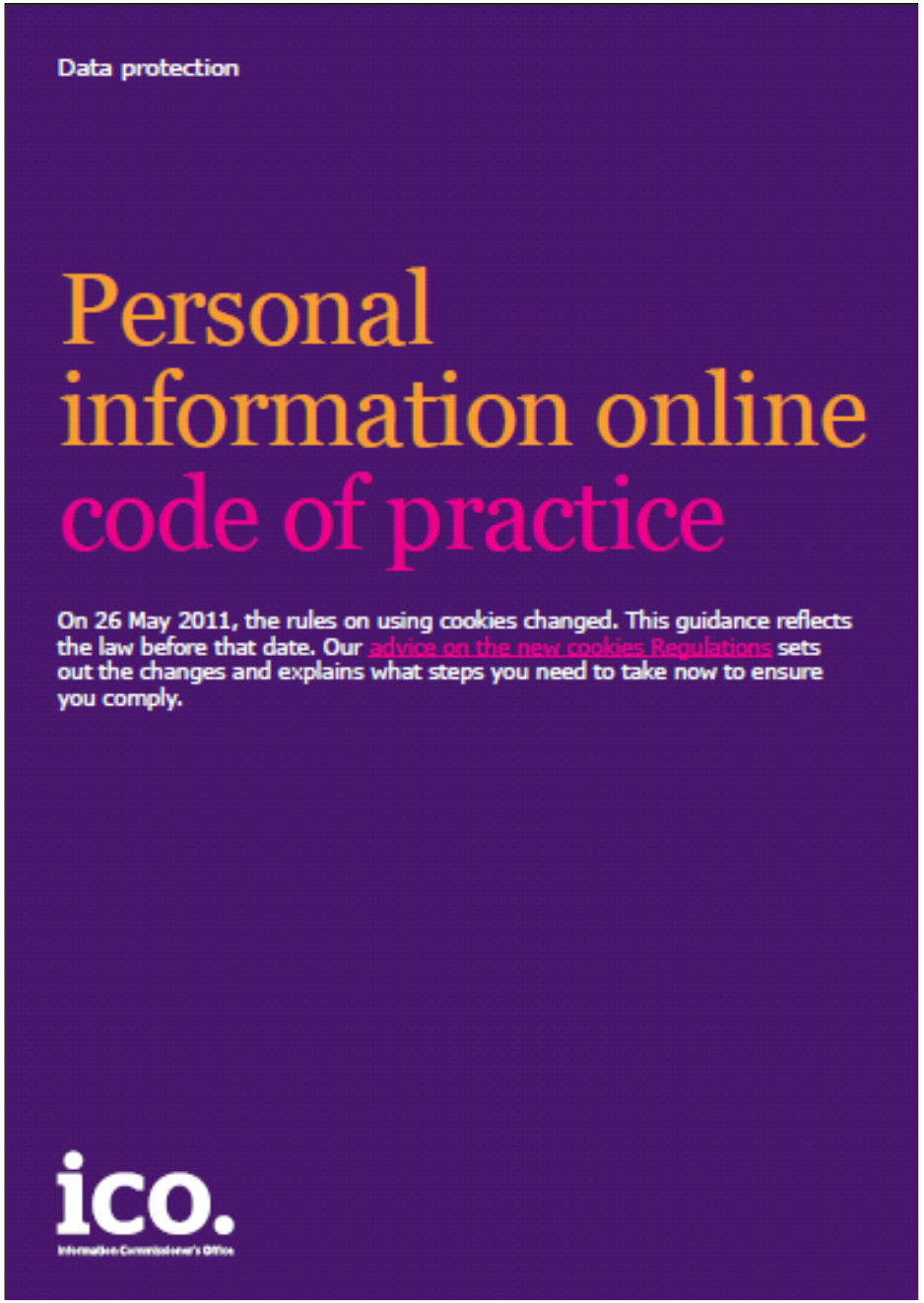
Thinking about a move to the cloud?

- Conduct a risk assessment before contracting with an online services company
  - What security do they offer?
  - What are the T&C's / SLAs?
  - Can I get my data out?
- Look at your data:
  - How will is be accessed?
  - Where will is be accessed?

ico.
Information Commissioner's Office

Guidance

- Ask your cloud provider difficult questions…



ico.
Information Commissioner's Office

If your company is offering online services to other organisations, can you:

- provide written guarantees about your security arrangements?
- guarantee that data will only be processed in accordance with your clients' instructions, e.g. that it will not be retained for longer than instructed?
- guarantee that your staff are trained and vetted to suitable standards, wherever they are based?
- explain your capacity to deal with serious technological or procedural failures?
- explain your complaints and redress procedure e.g. do you offer compensation for loss or corruption of clients' data?
- explain the facilities you offer to maintain high data protection standards, even if you store data in a country with weak, or no, data protection law, or where governmental data interception powers are strong and lacking safeguards?
- provide your customers with copies of their information regularly, in an agreed format and structure, so that they hold useable copies of vital information at all times?

If you cannot answer these questions to your potential clients' satisfaction, you will be at a competitive disadvantage. If you comply with any relevant standards – e.g. security - make this clear on your website.

et-based

cess data in
aintain an

of its staff, wherever
rofessional

om a serious

rding complaints and
loss or corruption of

its security track

ction standards will be
ountry with weak, or
ntal data interception

egularly, in an agreed
le copies of vital

ncerns about a
company's ability to look after the information you are responsible for, you should not use the provider concerned and should seek alternatives.

ico.
Information Commissioner's Office

Can the issues be designed out?

- Privacy by Design
- Privacy Impact Assessment
- Do you **really** need the personal data?
- How long do you **really** need it for?
- Can you protect some or all of the (personal) data?

PbD: Cloud SaaS

- Privacy by default
  - Private profiles
- Transparency
  - Third party domains / cookies
- Delete inactive / dormant accounts
- Security
  - Forced HTTPS
  - Force strong passwords or allow 2FA
  - Restrict logon by IP address

ico.
Information Commissioner's Office

PbD: Mobile devices

- The very nature of the cloud enables remote and/or mobile access
- Need to make devices “safe to loose”
  - Secure storage when not in use
  - Remote wipe
  - Enforce strong passwords
  - Password expiration
  - Block failed password attempts
  - Trusted devices Time out locks
  - External, internal or DMZ?

ico.
Information Commissioner's Office

Summary

- Cloud means different things to different people
- Different implementations have different data protection issues
- Data controller must assess the risks and remain in control
- Data security and data location key DP issues
- Many issues can be resolved early in the system design lifecycle

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on…

facebook

twitter

www.twitter.com/iconews

YouTube

LinkedIn

ico.
Information Commissioner's Office