



---

# Cloud computing & Data Protection

Tim Turner

Act Now Training

**CIPFA meeting, 28/11/11**



# Agenda

---

- What is Cloud Computing?
- The main DP issues
- Some points to keep in mind
- A checklist for where to go next



# “Cloud”

---

- **IT clouds are not new**
- Many people have an online email account
- Some use Hotmail as a business email:
  - fredbloggs@hotmail.co.uk
- I let Microsoft keep emails I don't print



# Cloud computing is...

---

- A cloud company owns servers world-wide
- Your software, data, services, computational power etc. is stored there
- They deliver these services to you via web
  - On subscription or
  - Pay-per-use



## (Sub) Contractors

---

- Cloud model includes a chain of contractors and sub-contractors
- You know your provider, but potentially not where your data is or who has it
- Inherent problem – you outsource the IT service but not the responsibilities



# Moment has come

---

- Steve Ballmer, CEO of Microsoft, says he is “**betting the company**” on cloud computing
- 70% of Microsoft’s R&D going into it
- Many organisations considering it



# Why do it?

---

- Cost reduction
- Staff reduction
- Outsourcing of staff and expertise
- Everything backed up
- Speed of access



# Cloud & DP

---

- Cloud has obvious DP implications
  - Transfer of data
  - Security of data
  - Access to data
  - You do not have your own data
- Danish DP Authority against use of cloud
- Problems in Germany too



# Obvious DP advantages

---

- **Back-up:** cloud model ensures your data is always available
- **Disaster recovery:** whole system separate from disasters at your place
- **Security:** virus, software and security options up-to-date can be part of service



# What does the ICO say?

---

- Personal Information Online code of practice, July 2010, is non-committal
- Main points:
  - Written contract required
  - Transfer data properly
  - Get security assurances
- Let's flesh that out!



# Think about DP principles

---

1 Info used fairly, lawfully, according to principles

Do you need to tell people?

How do you control access to your data?

2 Not re-used for incompatible purposes

3 Adequate, relevant, not excessive

Will the data always be available?

4 Accurate and up to date



# Think about DP principles

---

5 Retained for no longer than necessary

How do you know it's been deleted?

6 Used according to people's rights

7 Appropriately secure

This is a big one

8 Not transferred to country with inadequate protections

This is a big one



# Main DP concerns

---

- You have to transmit all of your data securely
- You have to get access to your data securely
- Provider has your data
  - what happens if their systems fail?
  - what if they go bust?
  - how do you control who else accesses your data?
  - how do you ensure your data is secure?



# BIG issue

---

- They are not legally liable for losses so you will need another lever to pull
- i.e. **financial penalties**



# At the beginning

---

- INVOLVE
- Your IT experts (for security standards)
- Your DP expert
- Your contract lawyers (if you don't have them, you need to buy in contract expertise)



# Pick your provider

---

- Cloud market has different slants
- Does your provider stress
  - Speed?
  - Cost?
  - **Security**
- Favour those who give security due weight
- ICO says look at security track record



# Pick your provider

---

- Do your 'Due Diligence'
- Where is your data likely to be?
- Some countries are considered safe
  - But what about Egypt? South Africa? China?
- What do they promise on location & security?



# The basics

---

- Use the EU approved model contract clauses **unaltered**
- Effect of contract must be that data is protected by UK standards, wherever it is



# Guarantees required

---

- You need guarantees
- Who gets access and in what circumstances?
  - Foreign governments with strong access powers
  - Subcontractors dispersed around globe
  - How is theft and illegal access prevented?



# Guarantees required

---

- What security is in place?
- Encryption
- Firewalls, hacking and virus protection
- Back-up
- Failure protection / prevention
- How is equipment disposed of?



# Guarantees required

---

- Are staff properly vetted and trained?
- Are incidents properly identified, reported and investigated?
- What compensation do you get for theft, corruption or loss?
- Will they pay your ICO fines?



# Practicalities

---

- How do you transfer the data?
- All personal and confidential data should be encrypted when transferred either way
- Your network connections need to be secure and reliable



# Wider issues

---

- Cloud computing may lead to a loss of IT expertise
- Relationship between you and cloud provider becomes asymmetric
- May dilute sense of responsibility for data



## Wider issues 2

---

- Big cloud providers already get attention from ‘hacktivists’
- They will never target you, but what about your cloud provider?



## Wider issues 3

---

- Cloud computing is trade off between direct control and cost & efficiency
- You surrender control, but IT is cheaper and more flexible
- It's for you to decide which wins out



---

# Contact Act Now for more advice and training

[www.actnow.org.uk](http://www.actnow.org.uk)

01924 451054