Revised Information Leaflet On Cloud Computing

Henry Chang
IT Advisor
The Office of the Privacy Commissioner for Personal Data

Why Cloud Computing?

	A	B	C
	Estimate on setting up a print shop		
		HK$ ('000)	
	B&W photo copiers	$ 200.00	
	Colour photo copiers	$ 100.00	
	On-sitediesel generator sets	$ 1,000.00	
	Ventilation alternation	$ 150.00	
	Qualified on-site engineers	$ 60.00	
	Fuel cost	$ 10.00	
	Hazardous licence application	$ 10.00	

Why invest on el ators when you can just plu wall?

IT servers and systems

cloud computing

What is Cloud Computing?

Gartner's Definition:

- **scalable and elastic IT capabilities**
- **provided as a service to multiple customers**
- **using Internet technologies**

Also

- **Low Opex and no Capex**
- **Green**

Cloud Computing Deployment Models

- **Deployment models**
  - **Public**
    - Google Apps for Business
    - Office 360
    - University email systems
  - **Community**
    - Amazon's cloud for the US Government
  - **Private**
    - Bank/Government's own clouds

Increased cost, control and flexibility for data users

Cloud Computing Deployment Models

- **Service models**
  - **SaaS (Software as a service)**
    - Providers provide virtual services (email, CRM)
  - **PaaS (Platform as a service)**
    - Providers provide virtual functional servers (database, webserver)
  - **IaaS (Infrastructure as a service)**
    - Providers provide cheap ‘virtual’ servers (simulated software servers derived from physical server) to customers

Increased overall cost, control and flexibility for data users

Characteristics of Cloud Computing Remain

- **With data storage across multiple jurisdictions so data moves across data centres dynamically and rapidly when spare capacity arises**

- **Cloud providers can flexibly engage (sub-)contractors to meet customer's elastic demands**

- **Standardised contract terms**

- **Share the same set of 'normal' outsourcing concerns**

Rapid Transborder Data Flow

Because many cloud providers now do tell and allow data user to choose storage locations…

Old Leaflet

- Would storage location be disclosed?
- Can storage location be specified?
- Do data users know overseas storage implications?

New Leaflet

- Implications of transborder data flow
- Cloud provider should disclose storage location and data users should know the implications
- Data users should select cloud providers that allow them to choose storage location

Loose Outsourcing Arrangements

Because a few cloud providers do disclose their outsourcing arrangements…

Old Leaflet

- Do data users know of the sub-contracting arrangement?
- Do protection and monitoring exist in sub-contracting arrangement?
- Do legal or contractual remedies exist?

New Leaflet

- Data users need to ascertain whether and how sub-contracting arrangement would protect the personal data they entrust to cloud providers

Standardised Contracts

Because there are more choices…

Old Leaflet

- Would cloud providers customise contracts?
- What monitoring options are available to data users?

New Leaflet

- Only use cloud providers that meet protection requirements
- Data users should make sure that they can verify compliance

Outsourcing Issues

There is actually no fundamental change…

Old Leaflet

- Outsourcing of personal data process does not mean outsourcing legal liability

New Leaflet

- Outsourcing of personal data process does not mean outsourcing legal liability

The ISO 27018 ‘standard’ for cloud providers

1. Not a ‘standard’ but a ‘guidance’ for cloud providers

2. Contains two parts

   A. IT security
      - Providing additional guidance specific to cloud providers in each of the 14 ISO 27002 IT Security controls
      - Therefore expecting cloud provider to meet ISO 27002 on IT security

   B. Privacy protection principles
      - Providing additional guidance specific to cloud providers in each of the 11 ISO 29100 privacy principles

The ISO 27018 ‘standard’ for cloud providers

Impacts of the ISO 27018 to the cloud industry:

1. **The first international standard for the cloud industry – should be a game changer.**
2. **Lots of marketing messages flying around about ISO 27018 and its certification.**
3. **It will create pressure for some others to follow.**
4. **It’s not a trivial requirement. Some providers will choose to comply and some won’t.**
5. **Impact likely towards cloud providers targeting enterprises but not SME/individuals.**
6. **Effects are still too early to assess.**

The ISO 27018 'standard' for cloud providers

Is the ISO 27018 a 'gold' standard?

1. The ISO 27002 IT security part is quite mature and the IT industry has many years' experience on how to comply and understand what the value and limits are;

2. The ISO 29100 privacy principle part is quite new. Furthermore, the ISO 27018 contains, for example:
   - A. Loose requirements:
     - Cloud provider to promptly notify data breach incidents.
   - B. 'Hen and egg' requirements:
     - Cloud provider contract should include minimum measures to ensure the contracted security arrangement are met.
   - C. 'Silver' standard:
     - Cloud provider to disclose storage locations and customers only have the option to terminate.

The ISO 27018 ‘standard’ for cloud providers

Final words

1. Compliance to ISO 27018 is not a demonstration of an absolute standard

2. Data user should still need to study the contract to make sure that the ‘degree’ of measures offered meet its requirements


Q
&
A