

Revised Information Leaflet On Cloud Computing

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



Why Cloud Computing?



	н		В	L
	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	
L	Fuel cost	\$	10.00	
2	Hazardous licence application	\$	10.00	
3				



Why invest on el-

IT servers and systems

ators when you can just plud computing cloud computing



What is Cloud Computing?

Gartner's Definition:

- scalable and elastic IT capabilities
- provided as a <u>service</u> to <u>multiple</u> customers
- using <u>Internet</u> 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)
 - laaS (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 subcontracting 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



OUTSOURCE

Standardised Contracts

Because there are more choices...

Old Leaflet

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

New Leaflet

- B. TITLE AND SURVEY
- In If Co. does worker? If the contract we want to be a proportion of the contract problem. If the contract problem is a limit of the contract problem is a limit of the contract problem. If the contract problem is the contract problem is the contract problem in the contract problem is the contract problem. If the contract problem is the problem in the problem is the problem in th
- 16. COMMITCHES PETCHES STITLE!
 The part of committee of the comm
- 11. CRED The property shall be transformed from Tabler to Prunhaser by manners of a Warnerby Owel, with Lian Comment, or Owersent, or Owel, contraved by the Safet. The Good and was property transfer game tax addition will be proper prepared and agreed on that I will be assigned for recording by the Country Comit in the Country to Santa the property is located. If it is not country to select the property as located. If it is not country to the country come in the Country to Santa the property is located. If it is not country to the country to the country to the country to which the property is located. If it is not considered the country to the country to
- beint in transferring to properly as an election, elementarily, trustee, contriblee, or conservator, the deed usual to such case shall be accepted. 12. NEW YORK STATE TRANSFER TAX, ADDITIONAL, TAX AND MONTOADE SATISFACTION.
- Tax prices are "Maries" tax or "Cultury term represent your new York or the 1 as use on terminals of a 1000,000 or town.

 15. NAX And CHEER ADJUSTMENDERS on the New Purchaser and Select are assuming the expenses of the property and not be a selected or the property of t
- Torse, sever, valer, refs., and condemnant or homeographic section has:
 Minright assessment year freatherns control assested in Non-TUT.
 Fut, seed on the market value at time of course, as sunfirmed by a sentification provided by Settler's augstine.
 Modern OF INSTRETAIN ADMINISTRATION.
- Impeditor of the properly of a resecution has, either of hours price to broade of this.

 RAMPERCO OF THIS PROSESSION

 The treated of this to the properly from Sales to Purchase will take gives of the office of the forder's allowing if the Turchologies and the office of the solution of the distinct for the solution of the
- No. of section 1. The control of the

Page 2 of 4 Purchaser's Initials Beller's Initials

- 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



- 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



Protect, Respect Personal Data

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.



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 <u>minimum</u> 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.



13

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











PCPD.org.hk