"Building Trust in the Cloud Era - Protect, Respect Personal Data"

Cloud Expo Asia Keynote Theatre

Cloud Expo Asia, Asia World Expo, Hong Kong

Stephen Kai-yi Wong
Barrister
Privacy Commissioner for Personal Data, Hong Kong

18 May 2016

Good morning ladies and gentlemen. I am delighted to join you in this Cloud Expo Asia and share with you some personal data privacy issues of cloud computing, from the point of view of a regulator.

2. Before I go into any details of the privacy concerns of using cloud, I need to lay some ground work first and explain the general legal requirements on data protection.

3. In this respect, I am pleased to tell you that the personal data protection regime in Hong Kong has been established for a long time. In fact, it was the first jurisdiction in Asia to enact the law in 1995 which then came into force in 1996. Not only was it the first in Asia, it was also a comprehensive piece of legislation covering both the private sector and the government, and is enforced by a statutory independent Commissioner.

4. The law itself meets international standard because it was modelled on the OECD (the Organization for Economic Cooperation and Development) privacy guidelines that was published in 1980. At the time of the bill's drafting, we also took note of the developing Data Protection Directive in the European Union. As a result, the Hong Kong Personal Data (Privacy) Ordinance is in compliance with both the OECD and the EU models.

5. Similar to the OECD Privacy Guidelines, the Hong Kong Personal Data (Privacy) Ordinance is principle-based and covers the entire personal data lifecycle of collection, retention, use and erasure. There are six data protection principles under the Ordinance.

DPP1

6. Data protection principle 1 concerns the collection of personal data which should be for a purpose related to the functions or activities of the data user. I should clarify here that data user means organisations or entities that collect personal data from individuals. Some jurisdictions call them data controllers but our law refer them as data users.

7. The means to collect personal data should be lawful and fair, and that personal data collected should be adequate and not excessive. In another words, the type of personal data and the means to collect it needs to be proportionate to the purpose.

8. For example, the collection of fingerprints purely for the purpose of ensuring punctuality at work is normally considered excessive.

9. When a data user collect personal data from a data subject (e.g. an individual or consumer), it is also required to duly inform the data subject, on or before the collection, the following information:

i. The purpose of the collection;
ii. To whom the collected personal data may be transferred;
iii. Whether it is obligatory or voluntary for the individual to supply the data, and if the supply of the data is obligatory, the consequence of not supplying the data; and
iv. The contact details of a person to whom access and correction requests of personal data may be made.

DPP2

10. Data protection principle 2 concerns the accuracy and retention of personal data. Data users should take all practicable steps to ensure collected personal data is accurate before using it.

11. Furthermore, since there must be a purpose for the collecting the personal data, when there is no longer a reason to keep the personal data, the personal data should be erased.

12. For example, the personal data of unsuccessful insurance applicant should not be retained by the insurer indefinitely just in case there will be dispute or for future reference.

13. I should add that the Ordinance has explicitly extended this last requirement on retention to any outsourcer handling personal data on behalf of

a data user. As cloud service providers are a form of outsourcers, the law requires the data user to use contractual, or other means, to ensure that the personal data it has entrusted to cloud service providers is not kept longer than necessary.

DPP3

14. Data protection principle 3 is about the restriction on using collected personal data for a new purpose. If a data user, after collecting personal data, wants to use it for a purpose other than the original or directly related purpose, the data user needs to obtain an express consent from the data subject before using the data for the new purpose. Similarly, data user needs to ensure that personal data it has entrusted to cloud service providers is not used for a new purpose by the cloud service providers without obtaining the requisite consent.

15. For example, the posting of compliant letter openly to show the personal data of complainants without their consent may be considered change of use and may contravene this requirement.

DPP4

16. Data protection principle 4 says that reasonably practicable steps must be taken by data users to ensure that there is no unauthorised or accidental access, processing, erasure, loss, use or transfer of the collected personal data. The principle further says that the kinds of data and the harm that any unauthorised action could result need to be taken into consideration when deciding what those reasonably practicable steps should be.

17. For example, the loss of USB drives with unencrypted personal data may be considered as a contravention because of the ease of loss of such devices so data users should encrypt the data to protect it against loss.

18. Similar to the Data Protection Principle 2, the Ordinance has explicitly extended this security requirement to any outsourcer handling personal data on behalf of a data user. So data user is required by the law to use contractual, or other means, to ensure that the personal data it has entrusted to cloud service providers is protected against unauthorised or accidental access.

DPP5

19. Data protection principle 5 on openness requires data user to take practicable steps to ensure data subjects can:

i. ascertain a data user's policies and practices in relation to personal data;
ii. be duly informed of the kinds of personal data a data user holds; and
iii. be informed of the main purposes for which personal data held by a data user are to be used.

20. For example, mobile apps accessing personal data of end-users should provide them with a privacy policy statement containing all these details.

DPP6

21. Last but not least, data protection principle 6 establishes the rights of data subject to ascertain whether a data user holds his personal data, and allows him the right to access to and correction of the personal data.

22. For example, after a patient has joined the recently launched Electronic Health Record Sharing System between the public and the private health care providers, the patent has the right to request access to the shared data stored in the system.

Cloud Computing and Personal Data Privacy Issues

23. Now that we know the requirements of the law, we can turn to the personal data privacy issues of cloud computing. Back in 2012 when cloud was an emerging technology, my Office produced a leaflet on what questions organisations should ask cloud service providers in order to understand how they would protect the personal data organisations entrust to them. Since then, the cloud market has matured a lot and in 2015, my Office updated the leaflet to advise organisations how they may select cloud service providers to store personal data.

International Views

24. The issues facing cloud computing when processing personal data is not unique only to Hong Kong so many of my colleagues worldwide have issued advice similar to my Office, including those by the EU's article 29 Working Party. The advice given in my Office's leaflet is consistent with those issued by these international bodies.

The Bottom Lines

25. Before I go into the privacy risks of clouds, I need to stress the bottom lines of engaging clouds. Simply put, organisations wanting to engage clouds need to remember that:

i. they need to be able to maintain control of the personal data;

ii. they are always fully responsible for the protection of the personal data; and

iii. the outsourcing of personal data processing does not mean they are also outsourcing the legal responsibility.

Three Privacy Risks

26. There are many potential privacy-related issues with cloud such as those related to the use of technologies such as virtualisation. But today I would concentrate on the risks associated with the business model of clouds, namely:

i. Rapid transborder data flow, where stored personal data may be moved from jurisdiction to jurisdiction by the cloud provider;

ii. Loose outsourcing arrangements where the cloud service provider may need to have many loose or informal outsourcing suppliers to support its operation yet the contractual relationship may be unclear; and

iii. Finally, many cloud service providers that are running on "high-turnover, thin-margin" business model only offer contracts to their customers with standard terms that may not meet the customer's minimum data protection requirements.

Rapid Transborder Data Flow

27. In terms of transborder data flow, many jurisdictions with data protection laws prohibit the transfer of personal data to jurisdictions without adequate or comparable data protection laws. Even in cases like Hong Kong where such provision is not currently effective, organisations holding personal data still owe to their customers or individuals the duty to protect personal data from data breach and mis-use.

28. Organisations that may have their personal data transferred to other jurisdictions must therefore be able to answer the "simple" questions of where the personal data will be transferred and whether those locations offer the same level of protection over personal data.

29. In the case of cloud, the very nature of its business model of optimising spare capacity means that data stored in clouds is liable to be moved from one location to another without the cloud customers' knowledge. This poses a problem for the cloud customer with personal data as it has the legal liability to ensure that personal data is stored in jurisdiction with comparable protection. If data user does not know where personal data is stored, it cannot even begin to assess the risk and the associated legal liability.

30. In order to deal with this risk, cloud service providers not only have to tell data users where their personal data will be stored, they really have to offer choices to data users to select where their personal data can only be stored.

31. Knowing and be able to choose which jurisdiction its personal data will be stored is only the first step. Once the storage locations are known, data

users need to assess compliance by checking whether they have obtained consent from individuals to store personal data there, whether such locations have comparable data protection laws or whether they haves exercised all due diligence to ensure that the personal data stored in the location will not be handled in ways that would be a contravention.

Loose Outsourcing Arrangements

32. In terms of loose outsourcing arrangement, it is believed that some cloud service providers that can offer flexible capacity is because they themselves are supported by many contractors with loose outsourcing arrangements so that they may meet the peak and trough demands of their customers. Some of these contractors may, in turn, supported by other sub-contractors. The problem with such loose contracting arrangements is that it is hard to ensure all controls required by the data user would appear and be enforced in the contracts between the cloud service provider and its first-level contractors or even second-level sub-contractors.

33. Very few cloud service providers are willing to be transparent about their contracting or sub-contracting arrangement but this practice could cause unacceptable uncertainty in terms of risks to be borne by the data user. Therefore if data user is to store personal data in the cloud, it should only engage cloud service providers that are transparent about their outsourcing practice. Naturally, even when cloud service provider is transparent about their outsourcing practices, data user will still need to ascertain if its data protection requirements are being enforced between the cloud service provider and its contractors and sub-contractors.

Standard Contract Terms

34. For convenience, cloud service providers that are running on "high-turnover, thin-margin" business model may tend to offer contracts to their customer with standard terms. However, data users must remember their legal liability and ensure that their data protection requirements are included in contracts. They must therefore assess if the contract contains all the data protection requirements in order to discharge their legal liability. If cloud service providers are not willing to change contractual terms to meet the needs of data user, data users should not be afraid to walk away.

35. Even in the cases where cloud service providers are willing to customise their contracts to suit the needs of data users, data users should then consider the next question on how they may ensure such customisation is being honoured. Given it is the legal responsibility of data users to ensure personal data stored in the cloud has the appropriate protection, data users really need to be given auditing right, or at least the ability to obtain third-party verification, on the fulfilment of contractual terms by cloud service providers.

Possible Solution to Using Cloud

36. Now that we have understood the personal data privacy issues on the use of clouds by data users, we need to look at how they may be addressed holistically.

Controls over Cloud Service Provider

37. For cloud service providers, the International Standardization Organization issued the *ISO 27018 Code of practice for protection of*

personally identifiable information (PII) in public clouds acting as PII processors which is the first international standard addressing the protection of personal data in the cloud. This is a long-waited standard that sets useful guidelines on what controls a cloud service provider should establish in order to give assurance to its customers when they entrust personal data to it.

The Structure of ISO27018

38. The ISO 27018 standard essentially has two parts to it. The first part is a "customised" version of the generic security controls of the IT security standard ISO 27002. This part customises ISO 27002 and prescribes very specific security controls applicable for the cloud service providers to observe. Similarly the second is a "customised" version of the generic privacy framework of ISO 29100. This part customised ISO29100 and prescribes very specific privacy controls applicable for the cloud service providers to follow. The result is simply a set of combined security and personal data privacy requirements that is specific to cloud service providers.

Some Specifics of ISO27018

39. To give some examples on what specific security controls and specific privacy control there are, I have listed here three such examples:

i. First, cloud service providers are required to be transparent and disclose to their customers the data storage locations;

ii. Second, cloud service providers are required to be transparent and disclose to their customers the outsourcing arrangements;

iii. Third, cloud service providers are required to make specific commitments to customers on not re-using personal data provided, on not retaining personal data longer than necessary, on personal data disclosure, on data breach notification, on minimum security and encryption etc.

The Obligations of Data User

40. However, I need to stress that the use of ISO27018 by the cloud service provider is only part of the equation. The ISO 27018 is definitely not a silver bullet, and using an ISO 27018 certified cloud service provider will NOT automatically make a data user compliant with the relevant data protection law.

41. A data user, having engaged ISO 27018 compliant cloud service providers, still needs to ensure that it has considered its obligations. For example, while it is the responsibility of the cloud service provider to disclose the storage locations and outsourcing arrangements, it is the responsibility of the data user to determine if there is any risk associated with storing personal data in the storage locations and allowing access by the contractors.

42. A data user may examine the data protection law and consider what it needs to do clause by clause but this "bottom-up" approach is a compliance-based, minimalist, approach to data protection that can easily fall short of the expectation of the public.

43. I therefore do not believe this is the only approach. Organisations should, as responsible corporate citizens, consider privacy from a broader management perspective and take into account factors such as corporate

reputation and respect for the privacy rights and expectation of their customers (the data subjects). We have been advocating that organisations should make personal data protection as part of their corporate governance responsibilities and implement it throughout their organisations using a top-down approach. This calls for a paradigm shift from compliance to accountability, which can be demonstrated by implementing a comprehensive privacy management programme (or PMP in short).

The Best Practice Guide

44. In order to achieve this, my Office released a guide entitled Privacy Management Programme: A Best Practice Guide in 2014.

45. The Best Practice Guide outlines what we advocate as good approaches for developing a sound PMP, which serves as a strategic framework to assist an organisation in building a robust privacy infrastructure to facilitate compliance with the requirements under the Ordinance. It also demonstrates the organisation's commitment to good corporate governance and building trust with its employees and customers through open and transparent information policies and practices.

46. The Best Practice Guide emphasises the importance of providing practical frameworks. Its key components included three top-down organisational commitments, seven bottom-up programme controls and a review process.

Three Top-down Organisation Commitments

47. In order to effectively comply with the legal requirements, organisations should cultivate a privacy respectful culture. The three top-down Organisation Commitments help facilitate this.

48. The first Commitment is to ensure top management buy-in of the PMP. Top management should be seen as committed to accountability and have a privacy management governance structure, including dedicating human and financial resources, endorsing the PMP and developing oversight. The second Commitment is the appointment of a Data Protection Officer or Office, who plays many roles with respect to personal data protection. The third top-down Commitment is to establish an internal reporting mechanism, so as to ensure the right people will know whether the PMP is functioning as expected.

Seven Bottom-up Programme Controls

49. On the other hand, the Best Practice Guide also identifies seven programme controls, which help to ensure what are mandated in the top-down commitments are implemented in the organisation.

50. Firstly, organisations should have a personal data inventory in place and be clear about what kinds of personal data they hold and where they are held. Organisations should know why they collect, use or disclose personal data and document these reasons.

51. Secondly, organisations should develop internal policies involving the collection of personal data, the accuracy and retention of personal data, the use of personal data including the requirements for consent, security of

personal data, transparency of organisations' personal data policies and access to and correction of personal data.

52. Thirdly, the proper use of risk assessment tools can help prevent problems. Such assessments should be conducted throughout the organisation for all new projects involving personal data and on any new collection, use or disclosure of personal data in ways that are materially different from existing practice. Organisations should develop a process for identifying and mitigating leakage and security risks, which could include the use of privacy impact assessments.

53. Fourthly, up-to-date training and education requirements for all relevant employees are essential to an effective PMP.

54. Fifthly, while reporting of major data breach to the Commissioner is not mandatory under the Ordinance, the Commissioner encourages organisations to adopt a procedure of notification in handling a data breach.

55. Sixthly, organisations should understand the importance of outsourcing or data processor management and impose obligations for data processor to take security measures. Also, organisations should ensure data processor will return, destroy or delete personal data when data is no longer required.

56. Lastly, organisations should take all practical steps to communicate with employees and customers, so as to ensure employees and customers can ascertain the organisations' personal data policies and practices

The Review Processes

57. The Best Practice Guide also discusses how to maintain and improve the PMP on an ongoing basis. A PMP should never be considered as an end product; it requires ongoing assessment and revision in order to be effective and relevant. The framework should be regularly monitored, assessed and updated as necessary to keep pace with changes both within and outside the organisation. This may encompass changes in such areas as technology, business models, law and best practices.

The Paradigm Shift

58. The PMP facilitate a paradigm shift in organisations that move them from a compliance approach to an accountability approach. Not only it makes an organisation proactive and preventative, it also allows an organisations to be more customer and reputation focused when it comes to the protection of personal data.

59. This paradigm shift is particularly important when it comes to the current age of cloud, big data and Internet of Things because it can shift the mind-set of the concerns on deploying these technologies with personal data as a potential liability to being an asset for an organisation to differentiate it from its competitors.

60. Enforcement and compliance remain an important aspect of ensuring personal data of individuals is being protected. In addition, the end result being winning trust from individuals/data subjects, the ability of organisations to demonstrate accountability would help cultivate and nourish the culture of "**Protect** and **Respect** personal data".

61. Thank you very much.