香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Information Leaflet

Cloud Computing

Introduction

This information leaflet aims to advise organisations which are considering engaging cloud computing on the factors they should consider. It explains the relationship between the cloud computing business model and the Personal Data (Privacy) Ordinance ("**the Ordinance**"). It highlights the importance for a data user to fully assess the benefits, risks and implications for privacy and data protection.

What is cloud computing?

There is no universally accepted definition for cloud computing but it is generally referred to as a pool of on-demand, shared and configurable computing resources that can be rapidly provided to customers with minimal management efforts or service provider interaction. The cost model is usually based on usage and rental, without any capital investment.

Typically there are three types of cloud computing service models; the infrastructure as a service (**IaaS**), the platform as a service (**PaaS**) and the software as a service (**SaaS**):

IaaS – Cloud providers provide basic computing infrastructure (such as CPU power, network bandwidth and storage capacity) to customers who are responsible for installing their operating systems and applications on top.

PaaS – Cloud providers provide basic computing infrastructure and platform (such as operating system, databases and web servers) to customers who are responsible for installing their applications on top.

SaaS – Cloud providers provide basic computing infrastructure, platform and applications (such as email systems, human resource and customer relationship management systems) to customers who will simply use the applications.

In terms of deployment, cloud computing may have the following models:

Private – Private clouds are set up for the exclusive use by a single customer or entity. It may be owned, managed and/or operated by the customer, a cloud provider or a combination of the two. It may be hosted on or off the customer's premises.

Community – Community clouds are set up for a group of customers or entities who often share the same concerns such as policy, security and compliance consideration. It may be owned, managed and/or operated by one or more of the customers in the community, a cloud provider or a combination of them. It may be hosted on or off the customer's premises.

Public – Public clouds are set up for the use by the general public including organisations. It may be owned, managed and/or operated by a cloud provider, an organisation or a combination of them. It is typically hosted on the cloud providers' premises.

Hybrid – Hybrid clouds are a combination of private, community and/or public cloud models put together for purposes such as disaster recovery or capacity overflow.

Regardless of which cloud computing service or deployment model is used, if data stored in the cloud includes personal data then it is the data user's responsibility to safeguard the personal data according to the requirements under the Ordinance.

Cloud computing engagement and the Ordinance

A data user shall comply with the requirements under the Ordinance including the data protection principles ("**DPPs**") in Schedule 1. In particular, DPP2(3), DPP3, DPP4 and Section 65(2) of the Ordinance are of particular relevance when engaging cloud providers.

DPP2(3) provides that when a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

DPP3 provides that personal data should not be used for a new purpose unless prescribed consent (i.e. express and voluntary consent) is obtained from the data subject or his/her "relevant person" as defined under the Ordinance.

DPP4(1) requires a data user to take all reasonably practicable steps to ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use, having regard to:

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

DPP4(2) provides that if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Section 65(2) of the Ordinance provides that any data breach or misuse of personal data by a data user's contractor (such as a cloud provider) shall be treated as carried out by the data user.

According to DPP2(3), DPP3, DPP4 and Section 65(2) of the Ordinance, data users are required to protect and prevent the misuse of personal data entrusted to them by data subjects regardless of whether such personal data is stored within the data users' premises, or outsourced to contractors or cloud providers.

Personal data privacy concerns

Some characteristics of the cloud computing business model (as opposed to the service model or the underlying technology) are of particular concern with regard to personal data privacy protection. These characteristics are:

1. Rapid transborder data flow

For cloud providers that have data centres distributed across multiple jurisdictions, personal data entrusted to them may flow from one jurisdiction to another regularly based on an algorithm that optimises the use of the cloud providers' storage and processing resources.

2. ***Loose outsourcing arrangements***

   Cloud providers may engage their own contractors. These contractors may further engage their own sub-contractors, in order to acquire the capacity and the speed necessary to meet customers' fluctuating computing demands. Such engagements may be based on loosely formed contracts or partnership, so as to remain flexible.

3. ***Standard services and contracts***

   Some cloud providers operate their business in a "quick turnover" and "thin margin" manner so that they only offer a small number of service types with standard contracts to their customers.

What should potential customers consider or find out before engaging cloud computing?

Data users considering storing personal data in the cloud, regardless of the type of service or deployment model used, should at least ensure that they have considered the following issues and their implications. As both the cloud computing technology and the market are evolving and maturing, not all cloud providers may address all the following issues effectively and provide satisfactory answers to these questions. Potential customers of cloud services are advised to challenge the cloud providers with these issues for a satisfactory assurance before they entrust personal data to the cloud providers.

Data users should note that these identified issues are by no means exhaustive. Data users shall exercise due care and diligence to explore the most suitable ways to comply with the Ordinance having regard to the characteristics and functions of cloud computing.

1. ***Rapid transborder data flow***

Section 33 of the Ordinance regarding the restriction against the transfer of personal data to places outside Hong Kong has not come into effect. However, if data users located in Hong Kong allow personal data collected by them to be transferred to places outside Hong Kong, they should ensure that such data is treated with a similar level of protection (as if it resides in Hong Kong) in order to meet the expectation of data subjects who entrust their personal data to them. Furthermore, data subjects who entrust personal data to them should be made aware of the transborder arrangement with regard to how their personal data is protected.

Potential customers of cloud services should consider:

1.1. Can the cloud provider disclose the locations/jurisdictions where the data will be stored so that this information is made clear to the data subjects? Are the data subjects aware of the implication of such storage (e.g. personal data that is transferred to another country is subject to the laws of that jurisdiction; no contract, no matter how well crafted, can override the laws of the foreign jurisdiction.)?

1.2. Can customers of cloud services specify personal data to be stored only in jurisdictions that they are reasonably certain that there are adequate legal/regulatory protection (e.g. the regulatory regime is substantially similar to Hong Kong)?

1.3. Do customers of cloud services know how overseas law enforcement agencies may have access to data stored in the cloud residing in their respective jurisdictions? Do they know if these authorities require judicial oversight as a safeguard against arbitrary data access?

2. Loose outsourcing arrangements

It may be common practice for some cloud providers to deliver service through contracting and sub-contracting. Data users using cloud service should be sensitised to such arrangements to ensure that their data protection requirements are still effectively complied with.

Potential customers of cloud services should consider:

2.1. Does the cloud provider have sub-contracting arrangements with other contractors? Would these contractors further sub-contract their work to others? Who among the employees of these cloud providers and their contractors/sub-contractors will have access to the personal data stored in the cloud? Is access restricted to those on a need basis? Are there appropriate authentication/access controls (and secured logging) in place? What measures are in place to ensure compliance with the data protection principles by these contractors/sub-contractors and their employees?

2.2. If sub-contracting arrangement exists, would all the data protection requirements in the contract between the customer and the cloud provider still be complied with effectively by these sub-contractors?

2.3. How can customers of cloud services ensure that the sub-contractors will offer the same level of protection as the cloud provider regarding the personal data put on the cloud?

2.4. If contractors/sub-contractors fail to protect the personal data put on the cloud, will they be subject to any contractual remedy or sanctions from their local regulatory authorities?

3. Standard services and contracts

When dealing with cloud providers that offer only standard services and contracts, data users must carefully evaluate whether the services and the contracts meet all security and personal data privacy protection standards they require. If there is a gap between what are being offered and what are required, data users must have the means to address the gap.

Potential customers of cloud services should consider:

3.1. If the standard security level or the personal data protection commitment by the cloud provider fails to meet customer requirements, would the provider customise its service to meet the requirements?

3.2. What practical steps can the customer of cloud services take to ensure that the level of security or personal data protection commitment will be honoured by the cloud provider? Would the provider provide independent verification on its practices and procedures to ensure they are in accordance with the agreement in place?

4. Other outsourcing issues

The concerns above are specific to the outsourcing arrangement of cloud providers. Since engaging cloud providers is considered as one form of outsourcing arrangements, the following general issues related to outsourcing would also have to be addressed.

4.1. Generally a data user can only enforce the provisions of the cloud contract against the cloud provider, and not the cloud provider's contractors/subcontractors;

4.2. Data users are ultimately responsible for the protection of the personal data collected and held by them. The outsourcing of any processing or storage of personal data to third-parties does not mitigate the data users' legal responsibility for the protection of the personal data they collect and hold. It may be problematic if the cloud provider is able to unilaterally change the agreement or limit its liability;

4.3. Data users have obligations under the Ordinance that include enabling customers to access their personal data, request corrections, and resolve issues and complaints. Accordingly, a data user must ensure that its contract with the cloud provider allows it to meet these obligations;

4.4. Data users should ensure that there is a provision in the contract with cloud providers to limit the use of personal data (and any other personal data cloud providers may collect during the course of the contract) to the original or directly related purposes of use at the time of data collection;

4.5. Data users should also ensure that there is a provision in the contract that sets out how personal data would be erased and/or returned to data users (or alternative providers) upon data user actions/requests, contract completion or contract termination;

4.6. Data users are recommended to impose in their contract with cloud providers an obligation on cloud providers to notify data breaches. Such mandatory notification by cloud providers would facilitate a timely handling of data breaches by data users, which includes ensuring speedy remedial action, business continuity, meeting legal obligations and public relations work. Data users should also ensure that this requirement is adhered to by the cloud providers' contractors/sub-contractors where applicable;

4.7. Data users need to ensure there is sufficiently clear and understandable notification in their personal information collection statement and/or privacy policy statement (or their equivalent) to inform the data subjects of their intention to outsource personal data processing to a cloud provider, that their personal data may be stored or processed in another jurisdiction, and that it may be accessible to law enforcement and national security authorities of that jurisdiction;

4.8. Data users are expected to ensure the same level of protection to personal data irrespective of whether the personal data is managed/held by them or by a cloud provider. In those cases where data users may not have direct oversight over all the controls necessary for the protection of personal data, they should seriously consider implementing a comprehensive and properly managed encryption system for the transmission and storage of personal data when engaging cloud services.

Furthermore, to assist data users in compliance with DPP2(3) and DPP4(2) when outsourcing the processing of personal data, the Commissioner has issued the publication "Outsourcing the Processing of Personal Data to Data Processors"[1] to which data users should refer.

[1] The publication is available at http://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Email : enquiry@pcpd.org.hk
Address : 12/F, 248 Queen's Road East, Wanchai, Hong Kong.
Website : http://www.pcpd.org.hk