Cloud Computing

This information leaflet aims to advise organisations on the factors they should take into account in considering engaging cloud computing. It explains the relevance of the Personal Data (Privacy) Ordinance (the "Ordinance") to cloud computing. It highlights the importance for a data user to fully assess the benefits and risks of engaging cloud computing and understand the implications for safeguarding personal data privacy.

What is Cloud Computing?

There is no universally accepted definition of cloud computing. For the purpose of this leaflet, it is 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.

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[1].

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.

[1] See further details of this requirement in the leaflet "Outsourcing the Processing of Personal Data to Data Processors" issued by the Privacy Commissioner for Personal Data (the "Privacy Commissioner"), available at www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf for details.

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[2].

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) will be treated as performed by the data user as well as by his contractor. In other words, a data user will be liable for the acts done by its contractor.

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 is outsourced to cloud providers.

Personal Data Privacy Concerns and How to Address Them

The personal data privacy concerns for data users in the use of cloud computing are largely related to the loss or lack of control over the use, retention/erasure and security of personal data entrusted to cloud providers.

Specifically, four control-related characteristics of the cloud computing business model are of particular concern with regard to personal data privacy protection[3].

Data users using cloud services are advised to obtain satisfactory assurance from the cloud providers to address these concerns before they entrust personal data to them.

These characteristics and how they should be addressed are detailed below:

I. 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 based on an algorithm that optimises the use of the cloud providers' storage and processing resources.

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[4].

[2] See footnote 1
[3] Data users should note that these identified issues are by no means exhaustive. Data users should exercise due care and diligence to ensure compliance with the Ordinance.
[4] See further details in the "Guidance on Personal Data Protection in Cross-border Data Transfer" issued by the Privacy Commissioner, available at: www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

Data users using cloud services should address the following issues:

- Cloud providers should disclose to data users the locations/jurisdictions where the data will be stored so that this information may be made known to data subjects. At the same time, data users need to consider their personal data privacy responsibilities with regard to such storage arrangement. For example, personal data that is stored in another jurisdiction is subject to the laws of that jurisdiction, and access by law enforcement agencies of the data in that jurisdiction may not have the same safeguards as in Hong Kong. Restrictions on data access as stated in a contract between data users and cloud providers cannot override the law of that jurisdiction.
- Data users should choose cloud providers that would allow them to choose/specify locations/jurisdictions where there is adequate legal/regulatory privacy protection to personal data (e.g. the regulatory regime is substantially similar to Hong Kong and that there is judicial oversight over law enforcement agencies against arbitrary data access).

II. Loose outsourcing arrangements

Cloud providers may engage their own sub-contractors. These sub-contractors may further engage their own sub-contractors in order to achieve the speed and acquire the capacity necessary to meet customers' fluctuating computing demands. Such engagements may often be based on loosely formed contracts or informal agreements.

Data users using cloud service should be sensitised to such arrangements and ensure that data protection requirements are still effectively complied with by such sub-contractors.

Data users using cloud services should address the following issue:

- Data users need to ascertain the sub-contracting arrangements of cloud providers. If there is a sub-contracting arrangement, data users should obtain formal contractual assurance from the cloud provider that the same level of protection (both technical and administrative) and compliance controls (monitoring and remedial actions) are equally applicable to their sub-contractors.

III. Standard services and contracts

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

When dealing with cloud providers that offer only standard services and contract terms, data users must carefully evaluate whether the services and the contract terms meet all security and personal data privacy protection standards they require. If there is a gap between what is being offered and what is required by data users, the gap must be addressed.

Data users using cloud services should address the following issue:

- If the standard security level or the personal data protection commitment by the cloud provider fails to meet customer requirements, data users should ask for customised service/contract terms that meet such requirements. Data users who fail to address the gap will bear the risks of data breach and misuse, and subject to regulatory scrutiny should such breach or misuse occur.

- Data users should find ways to verify data protection and security commitments made by cloud providers. If data users are given the right to audit the operation of cloud providers, they will have a first-hand knowledge of the compliance. While this is often not possible, and data users have to accept auditing reports or even claims of cloud providers, data users still need to scrutinise the scope, relevance and applicability of such reports or claims.

IV. Service and deployment models

Cloud providers' offerings include infrastructure as a service (IaaS), platform as a (PaaS) and software as a service (SaaS)[5]. Data users who use the IaaS and PaaS models tend to retain control over their business model and business tools they operate on. Data users who use SaaS, however, would have to use the software provided by the cloud providers as part of data users' business tools. Accordingly data users may have to adjust their operation in order to use such software or even rely on cloud providers to operate the software for them. As such, there could be less direct control by the data users over the personal data they are responsible for. Data users who use SaaS need to quantify the risks associated with such arrangement, and mitigate them according to circumstances.

Data users generally have a lot more control over dedicated private clouds than shared public clouds[6]. As such, any data user looking into the use of shared public clouds should assess carefully the issues identified in sections I to III above and seek ways to address them.

Other Outsourcing Issues

Since engaging cloud providers can be considered as one form of outsourcing arrangements, the following issues relating to outsourcing generally should also be addressed by the data user:

- 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 relieve the data users' legal responsibility for the protection of the personal data they collect and hold. Furthermore, it may be problematic if the cloud provider is able to unilaterally change conditions in the agreement it has with data users to a lower protection standard or limit its liability;
- 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 the data user to meet these obligations;
- Data users should ensure that there is 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) for a purpose which is the same as or directly related to the purpose of use at the time of data collection by the data users;
- Data users should also ensure that there is provision in the contract that sets out how personal data is to be erased or returned to data users upon data user requests, contract completion or contract termination;

[5] Cloud providers offering IaaS or PaaS may be considered as contractors offering physical servers or servers with operating systems installed. Customers of both services will need to further install and manage applications to use the service. SaaS on the other hand, includes functioning applications such as customer relationship management software, accounting software etc.

[6] Private clouds are set up by cloud providers for the exclusive use of a single customer and often are owned and managed by that customer. Public clouds, on the other hand, are set up, owned and managed by cloud providers for the shared use by the general public and businesses.

- Data users are recommended to impose in their contract with cloud providers an obligation on cloud providers to notify the data user of data breaches. Such mandatory notification by cloud providers would facilitate timely handling of data breaches by data users, which includes taking speedy remedial action, maintaining business continuity, meeting legal obligations and managing customer and public relations. Data users should also ensure that this requirement is adhered to by the cloud providers' contractors/sub-contractors, where applicable;
- Data users must ensure that there is sufficiently clear and comprehensible notification to customers in their personal information collection statement and/or privacy policy statement that personal data processing may be outsourced 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;
- Data users are expected to maintain the same level of protection of personal data irrespective of whether the personal data is managed/held by them or by a cloud provider. Where data users may not have direct oversight over all the controls necessary for the protection of personal data, they should seriously consider implementing an end-to-end, comprehensive and properly managed encryption system[7] for the transmission and storage of personal data.

The ISO Standard

The International Organization for Standardization (ISO) released the "*ISO/IEC 27018, a Code of practice for personally identifiable information (PII) protection in public clouds acting as PII processors*" ("the ISO 27018 standard") in August 2014[8].

This ISO 27018 standard covers the general principles and concerns regarding personal data privacy protection. It provides specific guidance for cloud providers in 14 security categories[9] defined under the commonly accepted IT security standard *ISO 27002 Code of practice for information security controls*, as well as the 11 privacy principles[10] described under the *ISO 29100 Privacy framework*[11].

It is beyond the scope of this leaflet to provide details of the ISO 27018 standard. Interested readers should study the standard themselves. Suffice it to say that data users must understand the limits of applicability of the ISO 27018 standard when engaging cloud providers who claim to be compliant with this standard.

While the ISO 27018 standard addresses the concerns identified in this leaflet, it does not mean data users engaging the ISO 27018 compliant/certified cloud providers are assured of compliance with the Ordinance. This is because, in some areas, the ISO 27018 standard specifies only what issues need to be addressed, but not how the issues should be resolved.

It will take time for this new standard to be properly understood and widely applied. However, the standard does provide a comprehensive reference that has met the need to assist the selection of cloud providers by data users.

[7] End-to-end encryption refers to an encryption system that only data users (but not cloud providers) have the ability to decrypt and understand the data.
[8] www.iso.org/iso/catalogue_detail?csnumber=61498
[9] Namely 1. Information Security Policies, 2. Organization of Information Security, 3. Human Resource Security, 4. Asset Management, 5. Access Control, 6. Cryptography, 7. Physical and environmental security, 8. Operation Security, 9. Communication security, 10. System acquisition, development and maintenance, 11. Supplier relationships, 12. Information security incident management, 13. Information security aspects of business continuity management and 14. Compliance.
[10] Namely 1. Consent and choice, 2. Purpose legitimacy and specification, 3. Collection limitation, 4.Data Minimization, 5. Use, retention and disclosure limitation, 6. Accuracy and quality, 7. Transparency and notice, 8. Individual participation and access, 9. Accountability, 10. Information security and 11. Privacy compliance.
[11] www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

Disclaimer

The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

First published in November 2012
July 2015 (First Revision)