Cloud computing in Hong Kong

7 SEP 2015
By: Scott Thiel | Edward Chatterton | Louise Crawford

The Hong Kong Privacy Commissioner for Personal Data ("PCPD") recently published an information leaflet outlining the application of the Personal Data (Privacy) Ordinance (the "PDPO") for data users looking to engage cloud providers. The information leaflet outlines the data protection principles ("DPPs") which apply in the context of cloud services, and highlights the particular characteristics of cloud computing that give rise to risks from a privacy perspective.

What is cloud computing?

While there is no universally accepted definition of cloud computing, the PCPD refers to it 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". In essence, it involves the storing and processing of data on computers in multiple locations, which are accessed over the internet. This differs from outsourcing which usually involves the customer's infrastructure being managed by a third party, and is also a departure from traditional software licensing or purchase of "on-premises" hardware.

The main benefit of cloud computing is that customers can avoid making the significant investment in IT infrastructure which would otherwise be needed in order to host large volumes of data. All they need is an internet connection, and this permits them to access their data from anywhere in the world. Cloud computing may also enable organisations to exploit other technologies that can give them a competitive advantage, such as big data analytics, which would otherwise be unmanageable given the magnitude and diversity of data involved.

Why does cloud computing engage data privacy law?

Cloud solutions can be used to process all kinds of data, but where that data is "personal data" (that is, it can be used to ascertain the identity of an individual), then the PDPO applies, and the interests of the following parties are engaged:

- **Data User**
  The entity or organisation that controls the collection and use of the personal data, and that chooses to adopt cloud services as part of its data management strategy.

- **Data Subject**
  Any individual whose personal data is being processed via the cloud services, e.g. an organisation's customer or employee.
• **Data Processor**
  The entity that provides cloud services.

Under Hong Kong law (and indeed in many other legal systems), responsibility to comply with privacy law rests with the data user, regardless of the action or inaction taken by the data processor. Accordingly, when engaging a cloud service provider, the data user should be mindful that responsibility for any breach of the PDPO lies with the data user, even if the breach is caused by the cloud service provider.

As a corollary of this, data users should select their cloud providers carefully, impose robust obligations upon them in relation to processing personal data, and obtain contractual indemnities in relation to any breaches. Taking these steps is not only important from a risk management perspective, but it also meets a statutory obligation under the PDPO: when engaging data processors, data users are required to use "contractual or other means" to ensure that:

i. personal data is not retained by the data processor for longer than is necessary (sometimes referred to as the "Retention Requirement"). This requires the data processor to comply with the data user's retention policy and to return (or destroy) personal data in its possession upon termination of the services; and

ii. personal data is protected against unauthorised or accidental access, processing, erasure, loss or use (sometimes referred to as the "Security Requirement"). The security measures necessary to meet the Security Requirement are not prescribed, however measures such as encryption, antivirus software, firewalls and physical security measures are considered best practice. The PCPD makes reference to the ISO 27018 Code of practice for personally identifiable information (PII) protection in public clouds acting as PII processors, which provides specific guidance for cloud providers, and may assist data users in selecting their cloud provider. However, as the PCPD makes clear, compliance with this standard is neither mandated by law, nor guaranteed to achieve compliance with the law.

**Personal data privacy concerns and how to address them**

Aside from the loss of control over the processing and storage of personal data, there are other factors which render cloud services "higher risk" from a privacy perspective. This does not mean that cloud services should not be used (and indeed, some cloud offerings could offer organisations enhanced protection compared with the measures that would otherwise be available in-house) but it does mean that appropriate steps should be taken to address these risks. The PCPD highlights the following unique "cloud" characteristics of which data users should be aware:
1. Rapid Transborder Data Flow

Cloud services are often provided from data centres located in multiple jurisdictions. This enables cloud providers to optimize storage capacity and speed of services. However, levels of physical and technical security may vary from country to country, and in some countries, the law may regulate levels of encryption, and possibly permit governments or regulators to mandate access to data. Accordingly, data users should ask cloud providers to disclose the location of their data centres, and cloud providers should only be engaged where they can demonstrate that data processed in overseas data centres will receive similar protection as if the data were in Hong Kong. Section 33 of the PDPO is not in force yet, however when this provision becomes effective (expected in the near future), data users will be restricted from transferring personal data outside Hong Kong unless a specific exception applies (e.g. where the data subject has consented in writing). Data users should carefully review their cloud arrangements to prepare for this section coming into force.

2. Loose outsourcing arrangements

Cloud services are often sub-contracted, and sometimes further sub-contracted again. The result is that data users have little visibility in practice, of where personal data is being processed, by whom, and what measures are being taken to protect it. Cloud service agreements should ensure control over sub-contracting. This means requiring the cloud provider to:

- give notice of sub-contracting (and in some circumstances, require the data user's approval);
- monitor and exert appropriate oversight over sub-contractors;
- permit auditing in respect of sub-contractors where this is required by the data user; and
- assume responsibility for any defaults of sub-contractors.

3. Standard services and contracts

Cloud services are often provided on standard form contracts, and in some cases these are said to be “non-negotiable”. The result is that cloud service contracts are often executed despite lacking key obligations which are required to ensure adequate protection of personal data. As a minimum, data users must ensure that undertakings are given in order to meet the Retention Requirement and the Security Requirement referred to above. In addition, the agreement should restrict sub-contracting and contain undertakings that will enable data users to comply with their regulatory requirements, for example, granting audit rights to comply with the data user's obligations in any regulatory investigation. In addition to scrutinizing the contract, due diligence should be conducted on the selected cloud service provider to ensure that the service provider has a good track record in terms of reputation and technical security. Moreover, some regulated institutions (e.g. banks and insurance companies) will be bound by industry regulations which impose additional risk management measures to be taken in relation to cloud service arrangements.

4. Services and deployment model

Certain cloud services are higher risk than others, depending on the type of service and deployment model. Broadly speaking, there are four types of clouds:

- **Public clouds**: Infrastructure, platform and software are provided through services accessible via online terms of use and paid for based on actual usage.
- **Private clouds**: Dedicated cloud computing resources are made available to the customer through negotiated service agreements. Because the resources are dedicated, capital investment may be greater.
- **Hybrid clouds**: This model may be used by a customer who desires the ease of use of a public cloud, but also wants some level of dedicated resources afforded by a private cloud.
- **Managed clouds**: This model is similar to outsourcing, but rather than having the customer own the infrastructure and outsource its management to a third party, the customer owns the cloud computing capability and outsources management to a third party.

Each of these methods can encompass the three basic cloud computing business models, including Infrastructure as a Service (IaaS) – where customers receive access to IT infrastructure often shared with others; Platform as a
Service (PaaS) – where customers can develop and operate applications by accessing a computing platform; and Software as a Service (SaaS) – where customers receive access to a suite of software applications remotely and on-demand.

Privacy risks tend to be higher where software is provided by the cloud provider (SaaS), particularly where software is being operated by the cloud provider (since software provides the tools to facilitate data processing requirements). The risks are also elevated where a public cloud is used, since data users have reduced control over the service. Data users should consider the deployment model to ensure that the service being provided is appropriate to their business, and that privacy risks are being managed.

**Other issues to consider in the procurement of cloud services**

Privacy is a key consideration when engaging cloud services, but there are other issues to consider too. Will this service meet business needs? Does this service provider have adequate capacity? How serious are the business consequences if there are service interruptions? The service level a customer receives from a cloud provider is either contained in the cloud service agreement, or it may be contained in a separate service level agreement incorporated by reference. Some considerations in developing service level agreements include:

- **Level of effort**: Customers should consider whether they require performance under the agreement to be absolute or subject to a less than absolute standard, such as “commercially reasonable efforts.” The level of effort on offer will vary from provider to provider.
- **Nature of obligations**: Most service level agreements focus on service availability, but service providers should also be prepared to respond to requests for specific commitments on performance, such as response times and bandwidth.
- **Definition of uptime**: Service level agreements should clearly define variables such as how uptime will be measured; what constitutes downtime; the nature of permitted downtime; and circumstances that do not constitute downtime.
- **Ability to suspend services**: A cloud service provider may at times need to suspend services, such as if a customer’s use of the services creates a security risk. While it may be reasonable for the provider to retain this right, it will be important for the customer to ensure that adequate notice is given.
- **Service credits**: The service level agreement should detail the amount of service credits available to customers, whether customers are automatically entitled to credits and whether there are circumstances under which the supplier is required to provide an actual refund.

**Recommended steps**

- Check existing contracts with your cloud providers and consider whether these arrangements comply with the law (and whether they will they continue to comply with the law when section 33 comes into force).
- Compile and regularly update a list of the names of cloud service providers and their sub-contractors, locations where cloud services are provided, and applications provided as part of the services. This will assist you with effective monitoring.
- Establish a negotiation strategy for selecting and engaging cloud service providers. Depending on the nature of your organization, some cloud service offerings may be inappropriate.
- Review privacy policies and personal information collection statements to ensure that appropriate notifications are given to data subjects in relation to the engagement of cloud providers.
- Consider whether a consent-based approach will need to be adopted for overseas transfers, in advance of section 33 coming into force.

If you have any queries or concerns about data privacy laws in Hong Kong or elsewhere, please contact the authors.

**AUTHORS**

Scott Thiel
Partner