Guidance on Cloud Computing

Introduction

This guidance highlights the factors that organisations should take into account when engaging in cloud computing. It explains the relevant requirements of the Personal Data (Privacy) Ordinance (the Ordinance) that are applicable to cloud computing and reminds organisations of the importance of fully assessing the benefits and risks of engaging in cloud computing and understanding its implications for personal data privacy.

What is cloud computing?

There is no universally accepted definition of cloud computing. Generally speaking, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cost model of cloud computing is usually based on usage and rental without any capital investment.

Cloud computing engagement and relevant requirements under the Ordinance

A data user (namely, the organisation that deploys cloud computing) must comply with the requirements under the Ordinance, including the **data protection principles** (DPPs) in Schedule 1 when holding, processing[1] or using[2] personal data. Special attention should be given to the requirements under **DPP2(3), DPP3, DPP4** and **Section 65(2)** of the Ordinance when engaging cloud service providers.

[1] "Processing" is defined in s.2 of the Ordinance to include, in relation to personal data, amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.

[2] "Use" is defined in s.2 of the Ordinance to include, in relation to personal data, the disclosure and transfer of the data.

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[3].

DPP3 provides that personal data must not be used for a new purpose unless prescribed consent (i.e. express and voluntary consent that has not been withdrawn) is obtained from the data subject or a "relevant person" (including parents or guardians) as defined under the Ordinance.

DPP4(1) requires a data user to take all reasonably practicable steps to ensure that any 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[4].

Section 65(2) of the Ordinance provides that any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated as done or engaged in by that other person as well as by the agent. In other words, any data breach or misuse of personal data by a data user's contractor (such as a cloud service provider) may, depending on the circumstances, be treated as performed by the data user as well as by the contractor. A data user may be liable for the acts done by the contractor.

According to DPP2(3), DPP3, DPP4 and Section 65(2) of the Ordinance, a data user is required to protect and to prevent the misuse of personal data entrusted to it by the data subjects regardless of whether such personal data is stored within the data user's premises or the storage of such data is outsourced to a cloud service provider.

---

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

[4] See footnote 3.

Personal data privacy concerns and how to address them

It is essential for data users to recognise the shared responsibility between data users and cloud service providers to safeguard data security in a cloud environment. This shared responsibility involves not only the initial assessment[5] of, and the assurance from, the cloud service providers[6] before the data users entrust personal data to them but also data users' and cloud service providers' actual compliance with the relevant privacy protection laws and requirements throughout the entire engagement.

From the perspective of data users, personal data privacy concerns arising from the use of cloud computing largely relate to their loss or lack of control over the use, retention, erasure and security of personal data entrusted to cloud service providers.

Due consideration should be given to four characteristics of the cloud computing business model that are particularly relevant to personal data privacy protection[7]. These characteristics and how related privacy concerns should be addressed are detailed below:

I. Service and deployment models

The service models offered by cloud service providers include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[8].

Data users who use the IaaS and PaaS models tend to retain control over their business models and business tools. However, data users who use SaaS have to use the software provided by the cloud service providers as part of the data users' business tools. Accordingly, data users may have to adjust their operation to use such software or rely on cloud service providers to operate the software for them. In such circumstances, it would be more difficult for data users to exercise direct control over the personal data for which they are accountable. Data users who use SaaS need to assess the risks associated with such arrangements and mitigate them according to the actual circumstances. Cloud service providers may update their cloud services from time to time to offer new features or configurations. Therefore, data users should take note of such updates and take corresponding actions, including updating the relevant software and/or adjusting the appropriate configurations.

Regarding deployment models, dedicated private clouds generally allow data users to have more control and privacy than shared public clouds[9]. Any data user considering the use of shared public clouds should carefully assess the issues identified in Sections II to IV below and seek ways to address them.

---

5 When conducting an initial assessment, data users may consider leveraging well established control frameworks from internationally recognised certifications and standards. See the relevant parts of this guidance under "ISO standards" and "Other standards".

6 Cloud service providers may provide assurance (in the form of attestations) or certification reports from reputable or internationally recognised third parties.

7 Data users should note that other considerations may apply in varying individual circumstances. Data users should exercise due care and diligence to ensure compliance with the provisions of the Ordinance.

8 Cloud service providers offering IaaS or PaaS may be considered as contractors offering physical servers or servers with operating systems installed, respectively. Customers of both services will need to further install and manage software or applications to use the service. In contrast, SaaS includes functioning applications such as customer relationship management software and accounting software.

9 Private clouds are set up by cloud service providers for the exclusive use of a single customer and are often owned and managed by that customer. In contrast, public clouds are set up, owned and managed by cloud service providers for shared use by the general public and businesses.

Preventing Unauthorised or Accidental Access or Processing

Data users should consider implementing the following measures to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data stored on the cloud:

- **Logging:** Data users should ensure that audit trails provided by cloud service providers are retained, such as user login history and personal data change history. Data users should review the logs regularly to detect abnormal activities. Audit trails will also facilitate investigations in the event of unauthorised access. Logs should be kept sufficiently secure so that intruders are unable to access and alter the log records to cover their tracks.

- **Appropriate user configuration:** Data users should thoroughly understand the functions of the configurations and ensure that their access to cloud services is correctly configured with reference to individual use cases. Furthermore, access should only be granted to authorised individuals, especially those who have operational needs to access the cloud services.

- **Separation:** Separation techniques can ensure that a data user's data cannot be accessed or affected by another client of the same cloud service provider. Data users should consider whether the measures implemented by cloud service providers are effective in ensuring that:

  (1) data users are able to control the access right to personal data stored on the cloud; and

  (2) their data and the cloud services are protected against malware executed by another client of the cloud service provider.

  To strengthen the protection, data users could consider leveraging logically isolated and multi-tenant computing services provided by the cloud service provider.

- **Encryption in transit and at rest:** Unprotected data, whether in transit or at rest, can expose an organisation to risks. As cloud computing provides services via the Internet, personal data should be encrypted during transmission to avoid eavesdropping or man-in-the-middle attacks. To protect data at rest, personal data should be encrypted when stored on the cloud to prevent unauthorised access from attackers, and it is also recommended that data users choose cloud service providers that offer encryption at rest in their services.

  Besides, the encryption keys for the transmission and storage of personal data need to be adequately protected and carefully managed to prevent the encrypted personal data from being easily accessed by unauthorised persons. If data users want to strengthen the control, they should consider implementing an encryption mechanism whereby only data users (and not cloud service provider) can decrypt and view the personal data.

- **Multi-factor Authentication (MFA):** MFA should be considered and enabled for as many accounts as possible, especially privileged account(s). The login steps could include two different factors listed below to enhance security:-
    - What you know – such as a password, or answers to security questions
    - What you have – such as a security token, or a smart card

- **Anonymisation:** Anonymisation provides an extra layer of security to the personal data stored on a cloud. Anonymising personal data means removing from the dataset any information from which an individual may be identified by anyone reading the record, taking re-identification risks into account.

- **Backup:** Effective backup and recovery policies and procedures should be developed by cloud service providers. For personal data stored on a cloud that are considered critical by data users, the data users should ensure that an offline backup copy of the data can be obtained from the cloud service providers and restored when needed.

- **Patch management:** Depending on the services and deployment models offered by cloud service providers, data users should ensure that cloud service providers have an appropriate patch management process in place to identify, assess, validate and apply necessary patches and security updates to safeguard the personal data stored on the cloud.

II. Standard services and contracts

Some cloud service providers operate their business in a "quick turnover" manner with a "thin margin" business model, offering only a small number of specific services to their customers on standard contract terms.

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

For example, data users using cloud services should address the following issues:

- **If the standard security level or the personal data protection commitment made by a cloud service provider fails to meet the data user's requirements, the data user should request customised services and negotiated contract terms that meet such requirements.** Data users who fail to address the gap would bear the risks and consequences of data breach and misuse, including regulatory scrutiny and reputational damage.

- **Data users should find ways to verify the data protection and security measures adopted by cloud service providers.** If data users are given the right to audit the operations of cloud service providers, they could acquire first-hand knowledge of the providers' level of compliance with the relevant personal data privacy requirements. As this is often not practicable in reality, data users should consider audit reports or declarations made by cloud service providers. Data users should carefully scrutinise the scope, relevance, reliability and authenticity of such reports or declarations.

III. Outsourcing arrangements

Cloud service providers may engage sub-contractors, who may in turn engage their own sub-contractors to quickly acquire the capacity necessary to meet customers' ever-changing computing demands. To maintain business agility, the outsourcing arrangements of some cloud service providers may be based on loosely formed contracts or informal collaborations.

Data users using cloud services should be alert to such arrangements and ensure that sub-contractors comply with the data protection requirements.

Data users using cloud services should address the following issue:

- **Data users need to ascertain the sub-contracting arrangements of cloud service providers.** If there is a sub-contracting arrangement, data users should ensure that they obtain contractual assurance from the cloud service 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. The cloud service provider should remain liable to the data user even where a breach of the terms of the agreement between the cloud service provider and the data user is caused by the cloud service provider's sub-contractors.

IV. Cross-border data transfers

Cloud service providers that have data centres distributed across multiple jurisdictions may transfer personal data entrusted to them from one jurisdiction to another to optimise their storage and processing resources. The decision to store or process personal data at offshore data centres should be made with careful consideration, as the handling of personal data stored at, or transferred between, offshore data centres may be subject to local laws of these jurisdictions.

Insofar as Hong Kong is concerned, when a data user transfers personal data to a place outside Hong Kong, they must comply with the relevant requirements of the Ordinance, including the six DPPs. In particular:

(a) When collecting personal data directly from data subjects, a data user intending to transfer personal data to a cloud server located outside Hong Kong should take all practicable steps to ensure that the data subjects are explicitly informed of the class of persons to whom the data may be transferred (i.e. the data recipients outside Hong Kong) and the purpose for which the data is to be used (DPP1).

(b) If personal data is transferred to a place outside Hong Kong for a new purpose[10], unless the transfer falls within the exemptions under Part 8 of the Ordinance, the prescribed consent[11] of the data subjects must be obtained for the transfer (DPP3).

If a data user engages a data processor to process personal data on its behalf in a place outside Hong Kong, the data user must protect the personal data by adopting contractual or other means to (i) prevent the personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP2(3)), and to (ii) prevent unauthorised or accidental access, processing, erasure, loss or use of such data (DPP4(2)).

It is recommended that data users refer to the following guidance materials of the Office of the Privacy Commissioner for Personal Data (the PCPD) concerning the cross-border transfers of personal data:

(a) *Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data*[12] (2022 Guidance) (published in 2022), including two sets of Recommended Model Contractual Clauses annexed thereto, which contain core provisions for cross-border data transfers that may be adopted by small and medium-sized enterprises;

(b) *Guidance on Personal Data Protection in Cross-border Data Transfer*[13] (published in 2014), including the Recommended Model Clauses annexed thereto, which contain a broader range of contractual clauses (in addition to the key provisions stated in the 2022 Guidance) in a cross-border transfer of personal data that may be more suitable for adoption by multinational corporations or organisations that are involved in complex cross-border transfers of personal data; and

(c) *Guidance on Cross-boundary Data Transfer: Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong – Hong Kong – Macao Greater Bay Area (Mainland, Hong Kong)*[14] (published in 2023), including the Standard Contract annexed thereto, which contains contractual clauses that may be adopted when a data user transfers personal data to a recipient registered (applicable to organisations) or located (applicable to individuals) in the nine Mainland cities within the Greater Bay Area (GBA)[15].

---

10 "New purpose" means any purpose other than the purpose for which the personal data was originally collected or for a directly related purpose.

11 "Prescribed consent" means consent that is expressly and voluntarily given and has not been withdrawn by the data subject in writing.

12 Available at: https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf

13 Available at: http://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

14 Available at: https://www.pcpd.org.hk/english/resources_centre/publications/files/standard_contract_gba.pdf

15 If a data user (registered or located in Hong Kong) and its cloud service provider (registered or located in the GBA) intend to transfer personal information from Hong Kong to a Mainland city in the GBA, the parties are encouraged to consider adopting the Standard Contract for such cross-boundary transfer.

Furthermore, data users using cloud services should address the following issues:

- **Cloud service providers should disclose to data users the locations/jurisdictions in which the data will be stored or processed, so that this information may be made known to the data subjects.** At the same time, data users need to consider their personal data privacy protection responsibilities with regard to such storage or processing arrangements. For example, personal data that is stored or processed in another jurisdiction is subject to the laws of that jurisdiction, and access of the data by law enforcement agencies 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 service providers cannot override the law of that jurisdiction.

- **Cloud service providers that have been selected should allow data users to choose or specify jurisdictions where there is adequate legal/regulatory protection of personal data** (e.g. the regulatory regime in those jurisdictions should be substantially similar to that of Hong Kong and there should be judicial oversight over law enforcement agencies to safeguard against arbitrary or unlawful data access).

Data subjects who entrust their personal data to data users should be made aware of the cross-border arrangements and how their personal data will be protected.

Other outsourcing issues

Because engaging cloud service providers can be considered a form of outsourcing arrangements, data users should generally address the following issues relating to outsourcing:

- Data users need to take ultimate responsibility for the protection of the personal data they collect and hold. **The outsourcing of any processing or storage of personal data to third parties does not reduce the data users' legal responsibility for the protection of the personal data which they collect, hold, process or use.** Hence, it would not be desirable for any cloud service agreement to permit cloud service providers to unilaterally amend its terms and conditions to provide a lower standard of protection or to limit its liabilities.
- **Data users have obligations under the Ordinance, including the requirements to provide customers with access to their personal data upon request, handle correction requests from customers and resolve problems and handle complaints.** Accordingly, a data user must ensure that its contract with the cloud service provider allows the data user to meet these obligations.

- **A data user should ensure that there are provisions in the contract with the cloud service provider to limit the use of personal data to the purpose(s) for which the personal data was originally collected by the data user or a directly related purpose** and should ensure that this limitation also applies to any other personal data that the cloud service provider may collect during the course of performing the contract.
- **When choosing cloud service providers, data users should carefully consider whether the physical hardware and cloud environment used by cloud service providers are secure to ensure adequate data protection. Data users should therefore obtain the relevant assurance from the cloud service providers or certification reports from third parties that are internationally recognised.** Once a data user transfers data to a data centre that it does not manage, security controls over the data are handed over to the cloud service provider. Anyone who has access to a data centre with multi-tenancy hosting will have the opportunity to access the physical devices holding the data of the cloud service provider's tenants. It is recommended that data users carefully evaluate whether the infrastructure and operating effectiveness of cloud service providers meet the security requirements of the data users.
- **A data user should ensure that there are provisions in the contract requiring the erasure or return of personal data held by the cloud service provider to the data user upon the data user's request, or at contract completion or termination.**
- **Data users should impose in their contract with cloud service providers an obligation on cloud service providers to notify data users of data breaches in a timely manner.** Such a mandatory notification by cloud service providers would facilitate the timely handling of data breaches by data users, which includes the giving of data breach notifications to the PCPD and affected data subjects, the taking of speedy remedial action and the maintenance of business continuity. This would enable data users to meet their legal obligations and effectively manage customer and public relations. Data users should also ensure that this requirement is adhered to by the contractors and sub-contractors (if applicable) of the cloud service providers.
- **Data users must ensure that clear and comprehensible notification is given to customers in their personal information collection statement and/or privacy policy statement that personal data storage and/or processing will be outsourced to a cloud service provider, and that their personal data may be stored or processed in another jurisdiction.**
- **If the personal data transferred to the cloud service providers will be stored or processed in jurisdiction(s) outside Hong Kong, data users should ensure that such cross-border transfers comply with the relevant cross-border requirements under the data protection laws of the relevant jurisdiction(s) and should seek professional legal advice if necessary.**
- Data users are expected to maintain similar levels of protection of personal data irrespective of whether the personal data is managed or held by themselves or by cloud service providers.

ISO standards

The International Organization for Standardization (ISO) has released a number of standards relevant to the use of cloud services:

(i) The *"ISO/IEC 27018:2019, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"*, last revised in 2019[16], establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. It also provides specific guidance for cloud service providers in 14 security categories[17] defined under *"ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls"*[18], as well as the 11 privacy principles[19] described under the *"ISO/IEC 29100:2024, Information technology – Security techniques – Privacy framework"*[20].

(ii) *"ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services"*, last reviewed in 2021, provides guidelines for information security controls applicable to the provision and use of cloud services[21].

(iii) *"ISO/IEC 27701:2019, Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines"*, released in 2019, specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation[22].

(iv) *"ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements"*, revised in 2022, specifies the requirements and provide companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation[23].

It is recommended that data users follow the relevant ISO standards which, depending on the circumstances of the case, the PCPD may take into account when assessing data users' compliance with the Ordinance.

---

16 https://www.iso.org/standard/76559.html

17 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

18 https://www.iso.org/standard/75652.html

19 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

20 https://www.iso.org/standard/85938.html

21 https://www.iso.org/standard/43757.html

22 https://www.iso.org/standard/71670.html

23 https://www.iso.org/standard/27001

Other standards

In addition to the above ISO standards, other standards that are relevant to the use of cloud services include the following[24]:

(i) GB/T 31167-2023 *Information security technology – Security guidance for cloud computing services* (信息安全技術　雲計算服務安全指南) published by the Mainland authorities;

(ii) GB/T 31168-2023 *Information security technology – Security capability requirements for cloud computing services* (信息安全技術　雲計算服務安全能力要求) published by the Mainland authorities;

(iii) Standards published by the United States' Department of Commerce's National Institute of Standards and Technology (NIST), such as *"Guidelines on Security and Privacy in Public Cloud Computing"*[25]; and

(iv) Standards published by the Singapore Information Technology Standards Committee (ITSC) under the Singapore Standards Council, such as SS 584:2020 (also known as Multi-Tier Cloud Security)[26].

It is beyond the scope of this guidance to provide details of the above standards. Data users may study the details of the standards and seek expert advice if necessary.

[24] Data users may also take note of the relevant requirements in the *"System and Organization Controls"* (SOC) issued by the American Institute of Certified Public Accountants. SOC is a suite of reports that Certified Public Accountants (CPAs) in the United States may provide in connection with the system-level controls of a service organisation or entity-level controls of other organisations. Relevant SOC reports will be produced during audits of an organisation's internal controls to provide information and assurance of the controls: https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

[25] https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing

[26] https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/industry-committees-and-working-groups/it-standards-committee

PCPD website
pcpd.org.hk

Download
this publication

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

PCPD.org.hk

Tel : **2827 2827**
Fax : **2877 7026**
Address : **Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

Disclaimer

The information and suggestions provided in this publication are for general reference only. This publication is not an exhaustive guide to applying 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 Privacy Commissioner for Personal Data (the Commissioner) makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided do not affect the functions and powers conferred upon the Commissioner under the Ordinance.

January 2025 (Second Revision)