Cloud Compliance Center - Hong Kong

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

Hong Kong

*This content was last reviewed around June 2023.*

**Cloud-neutral**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, provided that the financial institution meets all applicable legal requirements for the use of cloud services.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes.

The financial services regulatory regime in the Hong Kong Special Administrative Region of the People's Republic of China ("**Hong Kong**") is activity-based. It is possible that, depending on its activities, a financial institution could be supervised by more than one regulator. The primary regulators within the financial industry are the following:

The Hong Kong Monetary Authority ("**HKMA**"), which functions as the de facto central bank, is the prudential regulator and supervisor of banks, deposit-taking institutions, money brokers, issuers of certain stored-value facilities, and operators and settlement institutions of certain payment systems.

The Securities and Futures Commission ("**SFC**") is the principal regulator and supervisor of investment intermediaries such as brokers and fund managers operating within the securities and futures markets. The SFC also has regulatory oversight of Hong Kong Exchanges and Clearing Limited and The Stock Exchange of Hong Kong Limited.

The Customs and Excise Department ("**CED**") regulates the provision of currency exchange and cross-border remittance services.

The Insurance Authority ("**IA**") is the sole regulator of authorized insurers and licensed insurance intermediaries.

These Q&As focus on the HKMA's requirements for authorized institutions ("**AI**") and the SFC. The CED and IA may have additional or alternative requirements that should be considered by entities subject to their oversight.

**HKMA rules and regulations**

Entities regulated by the HKMA will be subject to various requirements on outsourcing, which include (but are not limited to) the following:

Module SA-2 of the Supervisory Policy Manual ("**SPM**") entitled "Outsourcing": This sets out the HKMA's supervisory approach to outsourcing and issues that an AI should address when outsourcing its activities.

SPM Module TM-G-1 entitled "General Principles for Technology Risk Management": This provides guidance on general principles that AIs are expected to consider in managing their technology-related risks.

SPM Module OR-1 entitled "Operational Risk Management" (version 25 July 2022) and SPM Module OR-2 entitled "Operational Resilience" (version 31 May 2022): This provides guidance to AIs on key elements of effective operational risk management and ensuring their operational resilience, including in relation to outsourcing.

Financial Institutions (Resolution) Ordinance, Code of Practice Chapter OCIR-1 on "Resolution Planning: Operational Continuity in Resolution" (version 5 November 2021): This sets out the expectations of the HKMA (in its capacity as resolution office for the banking sector) regarding the ex ante arrangements AIs should put in place (i.e., prior to resolution) to ensure the continuity of services that are essential to critical financial functions' performance and to support post-stabilization restructuring in a timely manner.

Circular dated 31 August 2022 entitled "Guidance on Cloud Computing": This sets out the HKMA's supervisory expectations on the adoption of cloud computing by AIs, including the engagement of third-party cloud service providers.

The HKMA also issues product- or service-specific materials, circulars, guidelines and supervisory documents (some of which may be issued directly to a financial institution and are only accessible to it) that also need to be considered for application on a case-by-case basis.

The HKMA may also provide AIs with internal guidance on outsourcing-related matters that is not publicly available.

**SFC rules and regulations**

Entities regulated by the SFC will be subject to various requirements on outsourcing, including some specific to the use of cloud services:

The International Organization of Securities Commissions ("**IOSCO**") Principles on Outsourcing of Financial Services for Market Intermediaries issued in 2005 ("**IOSCO Principles**"): The SFC has endorsed the use of these principles as the generally applicable standard to be complied with when a licensed corporation considers outsourcing its activities. The updated IOSCO Principles were published by IOSCO in 2021.

Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 ("**EDSP Circular**"): This sets out specific requirements (in addition to the IOSCO Principles) applicable to SFC-regulated financial institutions (other than banks) that use electronic data storage providers ("**EDSP**"). The EDSP Circular was supplemented in December 2020 by additional guidance in the form of frequently asked questions ("**EDSP FAQ**") and separate updated FAQ on premises for business and record-keeping. The EDSP FAQ provide further guidance on the following key aspects: (i) key personnel requirements for the purpose of the EDSP Circular; (ii) the application of the EDSP Circular where electronic regulatory records are kept with affiliates; and (iii) the use of undertakings by a designated manager(s)-in-charge/responsible officer as acceptable alternatives to undertakings being obtained from EDSPs.

Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission: These set out relevant internal control procedures in relation to the protection of, among others, a financial institution's operations and clients from financial loss arising from theft, fraud and other dishonest acts, professional misconduct or omissions.

Any other applicable circulars relevant to the activities undertaken by the licensed corporation

**Other requirements**

Any outsourcing will also need to be undertaken in accordance with relevant data privacy/security laws and regulations.

**3. Are there any specific contractual requirements for cloud outsourcing?**

Key requirements under both the Hong Kong Monetary Authority ("**HKMA**") and Securities and Futures Commission ("**SFC**") rules will vary based on the nature of the activities being outsourced and may include provisions in outsourcing agreements in relation to the following:

**Audit rights**: Broadly speaking, the financial institution (including its auditors), the HKMA and the SFC (as applicable) should be given access to information, records and other assistance as required.

**Use of subcontractors**: A notification to, or preferably prior approval from, the outsourcing institution should be required in advance of any further subcontracting of services by an outsourced service provider. The original outsourced service provider should remain responsible for and provide assistance to the outsourcing financial institution in the event of any problems with any subcontracted services.

**Technical and organizational measures or ICT guidelines**: Safeguards should be established to protect the integrity and confidentiality of customer information.

**Business continuity/disaster recovery**: A contingency plan for critical outsourced technology services should be developed to protect from any potential unavailability of services and ensure ongoing access to data due to unexpected problems (including, in the case of Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 and the electronic data storage providers FAQ, bankruptcy of the technology service provider).

**Termination rights**: Contractual termination rights should be clear and include a requirement for the service provider to assist with exit measures and transfer of information.

**Service levels and liabilities/guarantees/indemnities**: The type and level of services to be provided and the service provider's contractual liabilities and obligations should be clearly set out. Circular dated 31 August 2022 entitled "Guidance on Cloud Computing" or the HKMA Cloud Circular also requires the inclusion of clear provisions to address cloud-specific issues.

**Dispute resolution**: Provisions dealing with mechanisms to resolve disputes that might arise under the outsourcing arrangement should be clearly set out.

**Governing law**: The outsourcing agreement should preferably be governed by Hong Kong law (though this is not mandatory). For outsourcing on a cross-border basis, provisions dealing with choice of law should be included in any agreement as a matter of good practice.

**Customer data confidentiality**: Confidentiality obligations should be imposed on the service providers and their agents and, in the case of the SFC, an audit trail showing all access to any regulatory records (which includes customer data) should also be maintained.

**Payment arrangements**: These should be stipulated in the agreement as a matter of good practice.

**Regular review**: The agreement should provide for a regular review of the outsourcing arrangements, such that the financial institution can assess matters including whether the services are provided in accordance with any key performance indicators and the reasons for any failures to meet the agreed service standard levels.

The HKMA and SFC rules and regulations, along with the Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 and accompanying electronic data storage providers FAQ, also set out various additional granular requirements as to technical and organizational measures to be adopted, which may have implications for arrangements with cloud service providers.

**4. When does cloud outsourcing fall within the scope of the rules?**

Broadly speaking, engaging another party (which includes affiliates or head office) to perform functions that would otherwise be undertaken by a financial institution itself will be regarded as outsourcing.

**5. Does the outsourcing need to be notified to the regulator?**

If an authorized institution intends to outsource, it should first complete an internal assessment to identify the relevant risks posed by the proposed outsourcing and how they will be addressed, including an assessment to determine whether the outsourcing is "material" in nature. An outsourcing of a banking-related activity (including back office activities) or significant changes to the scope of an existing outsourcing of such activities is more likely to be material in nature and should be notified in advance to the Hong Kong Monetary Authority ("**HKMA**"). The HKMA will need to be satisfied that all the major issues set out in the Supervisory Policy Manual SA-2 entitled "Outsourcing" and any other applicable requirements are appropriately addressed. It may need to preapprove or provide a letter of no objection for the plan before it is implemented. The HKMA typically requires at least one month's advance notice, but a longer period is advisable.

**Securities and Futures Commission ("SFC")**

Where a licensed corporation regulated by the SFC proposes to keep regulatory records exclusively with an electronic data storage provider ("**EDSP**"), it will need to comply with the requirements of the Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 and EDSP frequently asked questions. These include the following:

Obtaining prior approval from the SFC for all the premises to be used for keeping such regulatory records

Providing the SFC with an EDSP undertaking or a manager(s)-in-charge/responsible officer undertaking and having all supporting materials, including a data access map, prepared and available upon request

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

Failure to comply with the Hong Kong Monetary Authority or Securities and Futures Commission (as applicable) requirements on outsourcing may negatively impact the ongoing assessment of the fitness and properness of the financial institution and the individuals involved in such noncompliance. This may result in disciplinary actions such as reprimands, fines or, at worst, a revocation of their license/authorization status.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes.

The Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("**PDPO**") governs the handling of personal data by data users, a similar concept to data controllers under the EU General Data Protection Regulation. The PDPO requires data users to comply with six Data Protection Principles ("**DPPs**"):

**DPP1** — Data Collection Principle. Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred, among other notification requirements. Data collected should be necessary but not excessive.

**DPP2** — Accuracy & Retention Principle. Personal data must be accurate and should not be kept for a period longer than is necessary to fulfill the purpose for which it is used.

**DPP3** — Data Use Principle. Personal data may only be used for the purpose for which the data was collected or for a directly related purpose, unless voluntary and explicit consent to a new purpose is obtained from the data subject.

**DPP4** — Data Security Principle. A data user needs to take all practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

**DPP5** — Openness Principle. A data user must make known to the public personal data policies and practices regarding the types of personal data it holds and how the data is used.

**DPP6** — Data Access & Correction Principle. A data subject must be given access to their personal data and be allowed to correct any inaccuracies.

However, if a cloud service provider is purely processing personal data on behalf of a financial institution as its customer and not for any of its own purposes, it would be considered a data processor and not a data user. Data processors are not directly regulated under the PDPO.

In such circumstance, the financial institution, as the data user, will remain liable for the actions or omissions of its authorized data processors (including the cloud service provider) and must monitor and control those data processors. Other requirements of particular relevance in a cloud context are that the financial institution, as a data user, would be obliged under the PDPO to adopt contractual or other means to ensure that the cloud service provider it engages does not retain data for longer than is necessary, and prevents unauthorized or accidental access, processing, erasure, loss or use of the data.

In practice, the regulator expects these requirements to be included as obligations in the written agreement with the cloud service provider, although a written agreement is not strictly mandatory.

As the PDPO is intended to be technology-neutral, there are no requirements that are specific to cloud services. However, the Privacy Commissioner for Personal Data has published an information leaflet on Cloud Computing (revised July 2015) ("**Leaflet**"), which provides an interpretation of how the DPPs apply to cloud service providers. The Leaflet sets out data privacy concerns in the cloud and how to address them. Key recommendations are as follows:

Cloud service 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.

Cloud service providers should be transparent on their subcontracting arrangements.

If the cloud service provider's security standards fail to meet customer requirements, customers could seek personalized terms with the cloud service provider.

Customers should have the right to verify data protection and security commitments/audit rights.

There is also a more general information leaflet on Outsourcing the Processing of Personal Data to Data Processors (September 2012). This provides guidance to data users on the use of data processors and recommendations for their engagement.

On the other hand, if the cloud service provider will be processing personal data for its own purposes (and not purely on behalf of its customer), it will be considered a data user under the PDPO and must comply with the PDPO's requirements, including the six DPPs.

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

Yes, but they are not in force.

There are restrictions on overseas data transfers in Section 33 of the Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("**PDPO**"). However, Section 33 has not entered into force and there are no indications that it will in the near future.

The Section 33 restrictions include limiting transfers to "white list" jurisdictions only (though there is currently no white list) and obtaining data subjects' consent to the transfer. The Hong Kong Privacy Commissioner has issued Guidance on Personal Data Protection in Cross-Border Data Transfer (December 2014), which serves as a practical guide to prepare for the implementation of Section 33.

In addition, the PCPD has issued more recent Guidance on Recommended Model Contractual Clauses for Cross-Border Transfer of Personal Data (May 2022), which includes recommended model clauses for cross-border transfers of personal data pursuant to Section 33(2)(f) of the PDPO, known as the "due diligence requirement" (though, again, Section 33 is not in force and, therefore, compliance with Section 33 is not legally required).

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No, provided the services do not constitute a licensed or regulated activity under, among others, the Banking Ordinance or the Securities and Futures Ordinance.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

They are not required from a privacy perspective, as long as the financial institution has explained to the data subjects (including its employees, if relevant) — in any relevant personal information collection statement or privacy policy provided on or before collection of their personal data — the purpose for which the cloud service providers will process their data and that their data will be transferred to a class of transferee that covers the cloud service provider. However, to the extent that a cloud service provider will process data for a "new purpose" not previously notified to the data subjects, under Data Protection Principle 3 of the Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong), the financial institution (as the data user) will need to obtain the data subjects' express consent.

As a matter of general customer confidentiality law, an authorized institution will generally need to obtain the customer's consent before it can disclose confidential customer information to another party (including a cloud service provider).

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

No.

However, please refer to the following response on legal obligations to disclose data.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes.

A cloud service provider must comply with lawful requests for disclosure of its customers' data from law enforcement agencies in accordance with Hong Kong laws. This means that, generally, it must disclose data, including personal data, to a government body or regulator in Hong Kong where required to comply with applicable laws or regulations, a court order, subpoena or other legal process, unless there are legal grounds to refuse. The Hong Kong Monetary Authority and the Securities and Futures Commission ("**SFC**") both have powers to request that third parties, such as cloud service providers, provide information in certain circumstances. In the case of the SFC, this disclosure requirement is specifically contemplated as part of the[Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019](https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59) ("**EDSP Circular**") and the electronic data storage providers FAQ.

**Interception and surveillance by law enforcement agencies**

The Interception of Communications and Surveillance Ordinance (Chapter 589 of the Laws of Hong Kong) ("**ICSO**") requires law enforcement agencies, including the police, the Immigration Department, Customs and Excise Department, and the Independent Commission Against Corruption, to apply for an authorization from either a designated judge or an officer of certain government departments to allow interception of communications. Under the ICSO, public officers may intercept communications where a "prescribed authorization" is obtained.

A prescribed authorization may require any person specified to provide to the department "such reasonable assistance for the execution of the prescribed authorization as is specified in the prescribed authorization," and Section 53 allows the commissioner on interception of communications and surveillance ("**Commissioner**") to require any person to provide to the Commissioner the content of intercepted messages or communications in their possession or control.

**National security law**

On 30 June 2020, the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**NSL**") came into operation in the Hong Kong Special Administrative Region ("**HKSAR**"). Broadly speaking, the NSL criminalizes four types of acts: (1) secession; (2) subversion; (3) terrorist activities; and (4) collusion with a foreign country or with external elements to endanger national security. The HKSAR Police Force has set up a designated department in charge of offenses endangering national security ("**National Security Offenses**"). Article 43 of the NSL empowers the police department to take specific measures when handling cases concerning National Security Offenses. These measures are in addition to the ones currently available under Hong Kong law for investigating serious crimes. The police department may require a person suspected on reasonable grounds of having in their possession information or material relevant to an investigation, to answer questions and furnish such information or produce such material. These measures require an order from the court of first instance.

**Telecommunications Ordinance (Chapter 106 of the Laws of Hong Kong)**

The powers of the Office of the Communications Authority, the Hong Kong telecommunications regulator, may give it incidental access to financial institutions' data held by a cloud service provider in certain circumstances (generally only to the extent that the cloud service provider is regulated under the telecoms licensing regime).

**Requests for disclosure from foreign governments and regulators**

There are no provisions under Hong Kong laws that oblige a Hong Kong-based cloud service provider to disclose data to a foreign government or regulator. The cloud service provider should first be satisfied that the overseas government or regulator has a valid legal basis to issue the request and that it has valid jurisdiction to request that the cloud service provider disclose data on its servers located in Hong Kong.

The cloud service provider should also refer to the relevant privacy policy of the financial institution to determine whether it is permitted to disclose to a foreign regulator or government entity personal data of the financial institution's customers that it may possess.

**Exemptions to privacy obligations under the PDPO**

The Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("PDPO") does not mandate the provision of personal data to a law enforcement agency or other body. However, the PDPO does list certain grounds that a data user may rely on as defense when disclosing a data subject's personal data without their consent for a new purpose (i.e., other than for a purpose originally notified to the data subject). One example is Section 58(1) PDPO, which relates to personal data held for purposes such as the prevention or detection of crime; the apprehension, prosecution or detention of offenders; the assessment or collection of any tax or duty; the prevention, preclusion or remedying of unlawful or seriously improper conduct, or dishonesty or malpractice; and the functions of a financial regulator.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, provided that the financial institution meets all applicable legal requirements for the use of cloud services.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes.

The financial services regulatory regime in the Hong Kong Special Administrative Region of the People's Republic of China ("**Hong Kong**") is activity-based. It is possible that, depending on its activities, a financial institution could be supervised by more than one regulator. The primary regulators within the financial industry are the following:

The Hong Kong Monetary Authority ("**HKMA**"), which functions as the de facto central bank, is the prudential regulator and supervisor of banks, deposit-taking institutions, money brokers, issuers of certain stored-value facilities, and operators and settlement institutions of certain payment systems.

The Securities and Futures Commission ("**SFC**") is the principal regulator and supervisor of investment intermediaries such as brokers and fund managers operating within the securities and futures markets. The SFC also has regulatory oversight of Hong Kong Exchanges and Clearing Limited and The Stock Exchange of Hong Kong Limited.

The Customs and Excise Department ("**CED**") regulates the provision of currency exchange and cross-border remittance services.

The Insurance Authority ("**IA**") is the sole regulator of authorized insurers and licensed insurance intermediaries.

These Q&As focus on the HKMA's requirements for authorized institutions ("**AI**") and the SFC. The CED and IA may have additional or alternative requirements that should be considered by entities subject to their oversight.

**HKMA rules and regulations**

Entities regulated by the HKMA will be subject to various requirements on outsourcing, which include (but are not limited to) the following:

Module SA-2 of the Supervisory Policy Manual ("**SPM**") entitled "Outsourcing": This sets out the HKMA's supervisory approach to outsourcing and issues that an AI should address when outsourcing its activities.

SPM Module TM-G-1 entitled "General Principles for Technology Risk Management": This provides guidance on general principles that AIs are expected to consider in managing their technology-related risks.

SPM Module OR-1 entitled "Operational Risk Management" (version 25 July 2022) and SPM Module OR-2 entitled "Operational Resilience" (version 31 May 2022): This provides guidance to AIs on key elements of effective operational risk management and ensuring their operational resilience, including in relation to outsourcing.

Financial Institutions (Resolution) Ordinance, Code of Practice Chapter OCIR-1 on "Resolution Planning: Operational Continuity in Resolution" (version 5 November 2021): This sets out the expectations of the HKMA (in its capacity as resolution office for the banking sector) regarding the ex ante arrangements AIs should put in place (i.e., prior to resolution) to ensure the continuity of services that are essential to critical financial functions' performance and to support post-stabilization restructuring in a timely manner.

Circular dated 31 August 2022 entitled "Guidance on Cloud Computing": This sets out the HKMA's supervisory expectations on the adoption of cloud computing by AIs, including the engagement of third-party cloud service providers.

The HKMA also issues product- or service-specific materials, circulars, guidelines and supervisory documents (some of which may be issued directly to a financial institution and are only accessible to it) that also need to be considered for application on a case-by-case basis.

The HKMA may also provide AIs with internal guidance on outsourcing-related matters that is not publicly available.

**SFC rules and regulations**

Entities regulated by the SFC will be subject to various requirements on outsourcing, including some specific to the use of cloud services:

The International Organization of Securities Commissions ("**IOSCO**") Principles on Outsourcing of Financial Services for Market Intermediaries issued in 2005 ("**IOSCO Principles**"): The SFC has endorsed the use of these principles as the generally applicable standard to be complied with when a licensed corporation considers outsourcing its activities. The updated IOSCO Principles were published by IOSCO in 2021.

Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 ("**EDSP Circular**"): This sets out specific requirements (in addition to the IOSCO Principles) applicable to SFC-regulated financial institutions (other than banks) that use electronic data storage providers ("**EDSP**"). The EDSP Circular was supplemented in December 2020 by additional guidance in the form of frequently asked questions ("**EDSP FAQ**") and separate updated FAQ on premises for business and record-keeping. The EDSP FAQ provide further guidance on the following key aspects: (i) key personnel requirements for the purpose of the EDSP Circular; (ii) the application of the EDSP Circular where electronic regulatory records are kept with affiliates; and (iii) the use of undertakings by a designated manager(s)-in-charge/responsible officer as acceptable alternatives to undertakings being obtained from EDSPs.

Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission: These set out relevant internal control procedures in relation to the protection of, among others, a financial institution's operations and clients from financial loss arising from theft, fraud and other dishonest acts, professional misconduct or omissions.

Any other applicable circulars relevant to the activities undertaken by the licensed corporation

**Other requirements**

Any outsourcing will also need to be undertaken in accordance with relevant data privacy/security laws and regulations.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

Key requirements under both the Hong Kong Monetary Authority ("**HKMA**") and Securities and Futures Commission ("**SFC**") rules will vary based on the nature of the activities being outsourced and may include provisions in outsourcing agreements in relation to the following:

**Audit rights**: Broadly speaking, the financial institution (including its auditors), the HKMA and the SFC (as applicable) should be given access to information, records and other assistance as required.

**Use of subcontractors**: A notification to, or preferably prior approval from, the outsourcing institution should be required in advance of any further subcontracting of services by an outsourced service provider. The original outsourced service provider should remain responsible for and provide assistance to the outsourcing financial institution in the event of any problems with any subcontracted services.

**Technical and organizational measures or ICT guidelines**: Safeguards should be established to protect the integrity and confidentiality of customer information.

**Business continuity/disaster recovery**: A contingency plan for critical outsourced technology services should be developed to protect from any potential unavailability of services and ensure ongoing access to data due to unexpected problems (including, in the case of Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 and the electronic data storage providers FAQ, bankruptcy of the technology service provider).

**Termination rights**: Contractual termination rights should be clear and include a requirement for the service provider to assist with exit measures and transfer of information.

**Service levels and liabilities/guarantees/indemnities**: The type and level of services to be provided and the service provider's contractual liabilities and obligations should be clearly set out. Circular dated 31 August 2022 entitled "Guidance on Cloud Computing" or the HKMA Cloud Circular also requires the inclusion of clear provisions to address cloud-specific issues.

**Dispute resolution**: Provisions dealing with mechanisms to resolve disputes that might arise under the outsourcing arrangement should be clearly set out.

**Governing law**: The outsourcing agreement should preferably be governed by Hong Kong law (though this is not mandatory). For outsourcing on a cross-border basis, provisions dealing with choice of law should be included in any agreement as a matter of good practice.

**Customer data confidentiality**: Confidentiality obligations should be imposed on the service providers and their agents and, in the case of the SFC, an audit trail showing all access to any regulatory records (which includes customer data) should also be maintained.

**Payment arrangements**: These should be stipulated in the agreement as a matter of good practice.

**Regular review**: The agreement should provide for a regular review of the outsourcing arrangements, such that the financial institution can assess matters including whether the services are provided in accordance with any key performance indicators and the reasons for any failures to meet the agreed service standard levels.

The HKMA and SFC rules and regulations, along with the Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 and accompanying electronic data storage providers FAQ, also set out various additional granular requirements as to technical and organizational measures to be adopted, which may have implications for arrangements with cloud service providers.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

Broadly speaking, engaging another party (which includes affiliates or head office) to perform functions that would otherwise be undertaken by a financial institution itself will be regarded as outsourcing.

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

If an authorized institution intends to outsource, it should first complete an internal assessment to identify the relevant risks posed by the proposed outsourcing and how they will be addressed, including an assessment to determine whether the outsourcing is "material" in nature. An outsourcing of a banking-related activity (including back office activities) or significant changes to the scope of an existing outsourcing of such activities is more likely to be material in nature and should be notified in advance to the Hong Kong Monetary Authority ("**HKMA**"). The HKMA will need to be satisfied that all the major issues set out in the Supervisory Policy Manual SA-2 entitled "Outsourcing" and any other applicable requirements are appropriately addressed. It may need to preapprove or provide a letter of no objection for the plan before it is implemented. The HKMA typically requires at least one month's advance notice, but a longer period is advisable.

**Securities and Futures Commission ("SFC")**

Where a licensed corporation regulated by the SFC proposes to keep regulatory records exclusively with an electronic data storage provider ("**EDSP**"), it will need to comply with the requirements of the Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019 and EDSP frequently asked questions. These include the following:

Obtaining prior approval from the SFC for all the premises to be used for keeping such regulatory records

Providing the SFC with an EDSP undertaking or a manager(s)-in-charge/responsible officer undertaking and having all supporting materials, including a data access map, prepared and available upon request

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

Failure to comply with the Hong Kong Monetary Authority or Securities and Futures Commission (as applicable) requirements on outsourcing may negatively impact the ongoing assessment of the fitness and properness of the financial institution and the individuals involved in such noncompliance. This may result in disciplinary actions such as reprimands, fines or, at worst, a revocation of their license/authorization status.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes.

The Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("**PDPO**") governs the handling of personal data by data users, a similar concept to data controllers under the EU General Data Protection Regulation. The PDPO requires data users to comply with six Data Protection Principles ("**DPPs**"):

**DPP1** — Data Collection Principle. Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred, among other notification requirements. Data collected should be necessary but not excessive.

**DPP2** — Accuracy & Retention Principle. Personal data must be accurate and should not be kept for a period longer than is necessary to fulfill the purpose for which it is used.

**DPP3** — Data Use Principle. Personal data may only be used for the purpose for which the data was collected or for a directly related purpose, unless voluntary and explicit consent to a new purpose is obtained from the data subject.

**DPP4** — Data Security Principle. A data user needs to take all practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

**DPP5** — Openness Principle. A data user must make known to the public personal data policies and practices regarding the types of personal data it holds and how the data is used.

**DPP6** — Data Access & Correction Principle. A data subject must be given access to their personal data and be allowed to correct any inaccuracies.

However, if a cloud service provider is purely processing personal data on behalf of a financial institution as its customer and not for any of its own purposes, it would be considered a data processor and not a data user. Data processors are not directly regulated under the PDPO.

In such circumstance, the financial institution, as the data user, will remain liable for the actions or omissions of its authorized data processors (including the cloud service provider) and must monitor and control those data processors. Other requirements of particular relevance in a cloud context are that the financial institution, as a data user, would be obliged under the PDPO to adopt contractual or other means to ensure that the cloud service provider it engages does not retain data for longer than is necessary, and prevents unauthorized or accidental access, processing, erasure, loss or use of the data.

In practice, the regulator expects these requirements to be included as obligations in the written agreement with the cloud service provider, although a written agreement is not strictly mandatory.

As the PDPO is intended to be technology-neutral, there are no requirements that are specific to cloud services. However, the Privacy Commissioner for Personal Data has published an information leaflet on Cloud Computing (revised July 2015) ("**Leaflet**"), which provides an interpretation of how the DPPs apply to cloud service providers. The Leaflet sets out data privacy concerns in the cloud and how to address them. Key recommendations are as follows:

Cloud service 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.

Cloud service providers should be transparent on their subcontracting arrangements.

If the cloud service provider's security standards fail to meet customer requirements, customers could seek personalized terms with the cloud service provider.

Customers should have the right to verify data protection and security commitments/audit rights.

There is also a more general information leaflet on Outsourcing the Processing of Personal Data to Data Processors (September 2012). This provides guidance to data users on the use of data processors and recommendations for their engagement.

On the other hand, if the cloud service provider will be processing personal data for its own purposes (and not purely on behalf of its customer), it will be considered a data user under the PDPO and must comply with the PDPO's requirements, including the six DPPs.

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

Yes, but they are not in force.

There are restrictions on overseas data transfers in Section 33 of the Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("**PDPO**"). However, Section 33 has not entered into force and there are no indications that it will in the near future.

The Section 33 restrictions include limiting transfers to "white list" jurisdictions only (though there is currently no white list) and obtaining data subjects' consent to the transfer. The Hong Kong Privacy Commissioner has issued Guidance on Personal Data Protection in Cross-Border Data Transfer (December 2014), which serves as a practical guide to prepare for the implementation of Section 33.

In addition, the PCPD has issued more recent Guidance on Recommended Model Contractual Clauses for Cross-Border Transfer of Personal Data (May 2022), which includes recommended model clauses for cross-border transfers of personal data pursuant to Section 33(2)(f) of the PDPO, known as the "due diligence requirement" (though, again, Section 33 is not in force and, therefore, compliance with Section 33 is not legally required).

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No, provided the services do not constitute a licensed or regulated activity under, among others, the Banking Ordinance or the Securities and Futures Ordinance.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

They are not required from a privacy perspective, as long as the financial institution has explained to the data subjects (including its employees, if relevant) — in any relevant personal information collection statement or privacy policy provided on or before collection of their personal data — the purpose for which the cloud service providers will process their data and that their data will be transferred to a class of transferee that covers the cloud service provider. However, to the extent that a cloud service provider will process data for a "new purpose" not previously notified to the data subjects, under Data Protection Principle 3 of the Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong), the financial institution (as the data user) will need to obtain the data subjects' express consent.

As a matter of general customer confidentiality law, an authorized institution will generally need to obtain the customer's consent before it can disclose confidential customer information to another party (including a cloud service provider).

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

No.

However, please refer to the following response on legal obligations to disclose data.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes.

A cloud service provider must comply with lawful requests for disclosure of its customers' data from law enforcement agencies in accordance with Hong Kong laws. This means that, generally, it must disclose data, including personal data, to a government body or regulator in Hong Kong where required to comply with applicable laws or regulations, a court order, subpoena or other legal process, unless there are legal grounds to refuse. The Hong Kong Monetary Authority and the Securities and Futures Commission ("**SFC**") both have powers to request that third parties, such as cloud service providers, provide information in certain circumstances. In the case of the SFC, this disclosure requirement is specifically contemplated as part of the [Circular to Licensed Corporations on Use of External Electronic Data Storage dated 31 October 2019](https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59) ("**EDSP Circular**") and the electronic data storage providers FAQ.

**Interception and surveillance by law enforcement agencies**

The Interception of Communications and Surveillance Ordinance (Chapter 589 of the Laws of Hong Kong) ("**ICSO**") requires law enforcement agencies, including the police, the Immigration Department, Customs and Excise Department, and the Independent Commission Against Corruption, to apply for an authorization from either a designated judge or an officer of certain government departments to allow interception of communications. Under the ICSO, public officers may intercept communications where a "prescribed authorization" is obtained.

A prescribed authorization may require any person specified to provide to the department "such reasonable assistance for the execution of the prescribed authorization as is specified in the prescribed authorization," and Section 53 allows the commissioner on interception of communications and surveillance ("**Commissioner**") to require any person to provide to the Commissioner the content of intercepted messages or communications in their possession or control.

**National security law**

On 30 June 2020, the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**NSL**") came into operation in the Hong Kong Special Administrative Region ("**HKSAR**"). Broadly speaking, the NSL criminalizes four types of acts: (1) secession; (2) subversion; (3) terrorist activities; and (4) collusion with a foreign country or with external elements to endanger national security. The HKSAR Police Force has set up a designated department in charge of offenses endangering national security ("**National Security Offenses**"). Article 43 of the NSL empowers the police department to take specific measures when handling cases concerning National Security Offenses. These measures are in addition to the ones currently available under Hong Kong law for investigating serious crimes. The police department may require a person suspected on reasonable grounds of having in their possession information or material relevant to an investigation, to answer questions and furnish such information or produce such material. These measures require an order from the court of first instance.

**Telecommunications Ordinance (Chapter 106 of the Laws of Hong Kong)**

The powers of the Office of the Communications Authority, the Hong Kong telecommunications regulator, may give it incidental access to financial institutions' data held by a cloud service provider in certain circumstances (generally only to the extent that the cloud service provider is regulated under the telecoms licensing regime).

**Requests for disclosure from foreign governments and regulators**

There are no provisions under Hong Kong laws that oblige a Hong Kong-based cloud service provider to disclose data to a foreign government or regulator. The cloud service provider should first be satisfied that the overseas government or regulator has a valid legal basis to issue the request and that it has valid jurisdiction to request that the cloud service provider disclose data on its servers located in Hong Kong.

The cloud service provider should also refer to the relevant privacy policy of the financial institution to determine whether it is permitted to disclose to a foreign regulator or government entity personal data of the financial institution's customers that it may possess.

**Exemptions to privacy obligations under the PDPO**

The Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("PDPO") does not mandate the provision of personal data to a law enforcement agency or other body. However, the PDPO does list certain grounds that a data user may rely on as defense when disclosing a data subject's personal data without their consent for a new purpose (i.e., other than for a purpose originally notified to the data subject). One example is Section 58(1) PDPO, which relates to personal data held for purposes such as the prevention or detection of crime; the apprehension, prosecution or detention of offenders; the assessment or collection of any tax or duty; the prevention, preclusion or remedying of unlawful or seriously improper conduct, or dishonesty or malpractice; and the functions of a financial regulator.

©Copyright © 2024 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.