Morgan Lewis | White Paper

WHAT YOU NEED TO KNOW ABOUT HONG KONG'S NEW RULES ON EXTERNAL ELECTRONIC DATA STORAGE

February 2020

www.morganlewis.com

The Hong Kong Securities and Futures Commission (SFC) has observed that the use of external electronic data storage providers (EDSPs), including public and private cloud storage, by licensed corporations (LCs) has become increasingly prevalent[1]. To address the increasing popularity of EDSPs, the SFC has published a circular (Circular) on October 30, 2019, setting out new requirements that LCs must comply with in storing and preserving the integrity of records or documents that LCs are required to keep under the Securities and Futures Ordinance (SFO) and the Anti-Money Laundering and Counter Terrorist Financing Ordinance (collectively, Regulatory Records) with EDSPs.

This paper (i) sets out a list of action points to assist LCs in determining to what extent the requirements in the Circular will apply to them, the timeline for making an application to the SFC (if needed), and an overview of the Circular; (ii) highlights the implementation issues in relation to the Circular; and (iii) sets out an implementation checklist on steps LCs can take now to implement the requirements of the Circular.

The industry continues to engage with the SFC to discuss the potential solutions to the practical implementation challenges. Hence, it is likely that there will be further developments, on which we will provide subsequent updates.

ACTION POINTS FOR LCs

Below is a list of questions to assist LCs in determining to what extent the requirements of the Circular will apply to them and the timeline for making an application to the SFC, if needed.

Definition of EDSPs: Do you use an EDSP[2] to store Regulatory Records? The consensus within the industry is that the Circular does not apply to storage of Regulatory Records with overseas intra-group affiliates (as further explained below) [3].

Exclusively and Nonexclusively: Do you store Regulatory Records *exclusively* or *nonexclusively* with an EDSP? This distinction is of critical importance as it determines the extent to whichthe Circular requirements will apply. Please refer to the section "Overview of the Circular – Exclusively and Nonexclusively," which considers this distinction.

Exclusively – SFC's Approval: If you store Regulatory Records exclusively with an EDSP you must apply to the SFC for approval. There are a number of stringent requirements that LCs must meet in order to obtain the approval, including (i) the appointment of two managers-in-charge *in Hong Kong* that, among other things, have the "knowledge, expertise and authority" to access all of the Regulatory Records (EDSP MICs) kept with the EDSP at any time; and (ii) depending on whether you use an HK-EDSP or Non-HK EDSP (both terms defined and explained below), you will need to submit a notice acknowledged by the HK-EDSP (the Notice) or an undertaking given by the Non-HK EDSP to the SFC (the Undertaking). These new requirements give rise to a number of implementation issues discussed below. We have also set out in Part I of the appendix a non-exhaustive list of the requirements LCs must comply with in order to make the application.

---

[1] SFC's Circular to Licensed Corporations – Use of External Electronic Data Storage, dated October 31, 2019.

[2] Please refer to the section, "Overview of the Circular – Definition of EDSPs" below for a complete definition of EDSPs.

[3] However, it is a broadly accepted interpretation within the industry that Section 130 of the SFO—which provides LCs must obtain the SFC's prior approval to use any premises to keep Regulatory Records—does apply to storage of Regulatory Records with overseas intragroup affiliates. The industry is discussing ways to deal with this issue, and we will keep readers updated on further developments in this regard. This paper will therefore not deal with intragroup storage.

Deadline for Applying for Approval: LCs that use an HK-EDSP must apply for approval and implement the requirements of the Circular by June 30, 2020, and LCs that use a Non-HK EDSP should try as much as possible to comply with the Circular, although the June 30, 2020, deadline does not apply. The SFC has not indicated whether it will give an extension of the deadline; however, if LCs encounter difficulties in preparing for the approval applications in light of some reasons, such as the coronavirus outbreak, LCs should contact the SFC as soon as practicable.

LCs that Use EDSPs Nonexclusively: These types of LCs do not need to apply to the SFC for approval.

New Internal Control Requirements – LCs that Use EDSPs Exclusively and Nonexclusively: LCs, regardless of whether they use EDSPs exclusively or nonexclusively, will still need to comply with additional internal control requirements and review their existing contractual agreements with EDSPs (as set out in Part E of the Circular). We have summarized these requirements under the section, "General Obligations of LCs using External Data Storage or Processing Services" below and provided practical guidance on implementing some of these requirements in Part II of the appendix.

OVERVIEW OF THE CIRCULAR

Under Section 130 of the SFO, LCs are required to seek the SFC's prior written approval for the use of premises for keeping records or documents relating to the carrying on of the regulatory activities for which they are licensed. However, until the publication of the Circular, it is not clear how the SFC's requirement to approve the recordkeeping *premises* would apply to, for example, cloud services, as arguably clouds are not premises (as this word is commonly understood).

The Circular clarifies the above and introduces a number of new requirements for LCs that use EDSPs to store Regulatory Records, whether on an exclusive or nonexclusive basis.

When reading the Circular, it is important to bear in mind the SFC's overriding objective – the need to present evidence in court. The SFC's key concern is in relation to preservation and prevention of tampering of Regulatory Records.

Definition of EDSPs

The SFC defines EDSPs to include external providers of

- public and private cloud services;
- servers or devices for data storage at conventional data centres;
- other forms of virtual storage of electronic information; and
- technology services whereby information is generated in the course of using the services and then stored at such service providers or other data storage providers, and such information can be retrieved by the service providers.

Interestingly, the SFC remains silent on whether storage of Regulatory Records with intragroup entities will fall within the definition of EDSPs or will be treated separately, subject to another set of requirements. This is unfortunate as this issue is of critical importance since most global financial institutions that operate in Hong Kong typically store Regulatory Records at servers (or through other electronic means) in a number of jurisdictions. Historically, the SFC stance was that while it would not approve overseas recordkeeping premises as the SFC may be precluded from exercising its statutory rights to access and inspect these records, it will be acceptable if the LCs kept identical copies of these

records that the SFC can access contemporaneously on the LC's approved recordkeeping premises. However, after the publication of the Circular, this approach is no longer tenable. The consensus within the industry is that the Circular does not apply to overseas intragroup affiliates and the industry is discussing ways to deal with this issue. We will keep readers updated on further developments in this regard.

The other issue is whether software as a service (SaaS), such as Salesforce will fall within the scope of the Circular. A number of financial institutions in Hong Kong use SaaS, and at the moment, there is no consensus within the industry on how the Circular would apply to SaaS. Again, we will keep readers updated.

Exclusively and Nonexclusively

As noted above, the Circular draws a distinction between LCs that keep Regulatory Records with EDSPs exclusively and nonexclusively.

Exclusively means where LCs rely exclusively on EDSPs for the storage of Regulatory Records and the LCs do not contemporaneously keep a full set of identical Regulatory Records at the LC's approved recordkeeping premises in Hong Kong.

Nonexclusively means where LCs keep a full set of identical Regulatory Records at SFC approved premises used by the LCs in Hong Kong – for example, where cloud storage is used only as a backup or the use of cloud computing services, but retain all Regulatory Records at their premises.

SFC's Approval of LCs That Use EDSPs Exclusively

LCs will need to fulfil the requirements in the Circular in order to make an application. We have set out the key requirements below, some of which give rise to implementation issues discussed in the next section:

- **Designation of Two EDSP MICs in Hong Kong**: The EDSP MICs in Hong Kong must have the knowledge, expertise, and authority to access all of the Regulatory Records kept within an EDSP at any time, who can ensure that the SFC has effective access to such records upon demand without undue delay in the exercise of its statutory powers. The EDSP MICs, or their delegates, must have in their possession all digital certificates, keys, passwords, and tokens to ensure full access to all Regulatory Records kept with the EDSP. The EDSP MICs will be responsible for ensuring information security to prevent unauthorised access, tampering, or destruction of Regulatory Records. This gives rise to a number of implementation issues, which are discussed below.
- **Notice/Undertaking to Be Given by EDSPs to the SFC**: If the EDSP is either a company incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance (HK-EDSP), it is necessary for the LC to send the notice to the HK-EDSP that will need to be acknowledged by the HK-EDSP (the Notice). If the EDSP is an overseas company (Non-HK EDSP), it is necessary for the Non-HK EDSP to give an undertaking (the Undertaking) to the SFC. The content of the Notice and the Undertaking gives rise to a number of issues discussed below.
- **Regulatory Records Must Be Accessible at All Times**: LCs must ensure all of their Regulatory Records are kept exclusively with EDSPs and are fully accessible upon demand without delay by the SFC, and can be reproduced in a legible form from LC premises.

- **Audit Trail**: LCs should ensure that they can provide audit trail information in a legible form regarding any access to the Regulatory Records (including read, write, and modify) stored by the LCs at the EDSPs. The audit trail should be a complete record of any access by the LCs to the Regulatory Records. The audit trail information should be kept for the period for which LCs are required to keep Regulatory Records[4]. The access to the LC audit trail information should be restricted to read-only and LCs should ensure that each user who has accessed Regulatory Records can be uniquely identified from the audit trail.
- **SFC's Access Power Must Not Be Impaired**: Regulatory Records must be kept in a manner that does not impair or result in undue delays to the SFC's effective access to the Regulatory Records when it discharges its functions or exercises its powers, taking into account all pertinent political and legal issues in any relevant jurisdiction.

IMPLEMENTATION ISSUES

Practical Challenges Around Production of Data

The Notice and the Undertaking require an EDSP to produce LC's data to the SFC in circumstances where the EDSP will not have access to the data itself and will not be able to identify the data responsive to the SFC's specific requests. This raises the issue of whether the SFC expects LCs to provide greater access to their data to EDSPs (including for example, by providing their encryption keys to EDSPs' staff) and, if so, this is likely to weaken the cybersecurity of LC's data by increasing the number of people with access to this data.

Against this backdrop, the SFC has said its primary concern is that data must be preserved and must not be tempered with. As such, the industry is currently working on a solution which can satisfy the SFC's objective of preserving and locking down the data.

Access to Data Without Notifying the LC

The Notice and the Undertaking requires an EDSP to provide any or all of the data relating to the LC, as required by the SFC pursuant to exercise of statutory power, without giving the LC any notification about such requirement having been received.

LCs are concerned with whether they will have any opportunity to assert legal professional privilege over any privileged material embedded in the data stored with EDSPs.

The SFC has said it is not trying to prevent LCs from asserting legal professional privilege and will continue to respect it. Again, the SFC has emphasized that its key concern is the need to present evidence to court, and hence preservation of records and prevention of tampering with the records. As such, the industry is currently working on a solution that can satisfy the SFC's concern.

Two Hong Kong EDSP MICs

There have been voices from the industry regarding the practical difficulties in appointing two appropriate individuals based in Hong Kong, especially for those LCs that have a small Hong Kong presence and a large presence offshore. The Circular requires the EDSP MICs or their delegates to have "in their

[4] Generally speaking, depending on the types of Regulatory Records, the record retention period is two, five, or seven years.

possession all digital certificates, keys, passwords and tokens to ensure full access to all Regulatory Records kept with the EDSP." However, in practice, for a global financial institution, such digital certificates, keys, passwords, and tokens are often kept by more senior people offshore.
This is one of the most contentious requirements under the Circular, and the industry is working very hard to try to reach a workable solution with the SFC.

Notice/Undertaking

It is uncertain whether EDSPs will in fact be willing to acknowledge the Notice (in the case of HK EDSPs) or sign the Undertaking (in the case of Non-HK EDSPs) as the SFC does not regulate EDSPs. The terms of the Notice/Undertaking are very onerous – for example, if the SFC or the Hong Kong Department of Justice initiates any proceedings, the staff members of the EDSP having technical knowledge of the operation of the electronic data storage or information system of the EDSP must provide certificates pursuant to Section 22(A) of the Evidence Ordinance or any other statutory provision certifying a number of matters as stated in the Notice/Undertaking. Such staff members may also need to give evidence in the proceedings.

It is also uncertain whether the SFC will accept material amendments to the Notice or the Undertaking.
As of the date of this writing, it is not clear whether any EDSP will enter into such Notice/Undertaking, which is needed if the LCs that rely on EDSPs exclusively want to make an application to the SFC.

GENERAL OBLIGATIONS OF LCs USING EXTERNAL DATA STORAGE OR PROCESSING SERVICES

Regardless of whether LCs use EDSPs exclusively or nonexclusively, it is crucial for LCs to comply with the general obligations of using electronic data storage or processing services as set out in Part E of the Circular, including the following:

1. Conducting proper initial due diligence on the EDSP and its relevant controls and regular monitoring of the EDSP's service delivery. Such due diligence should cover, among others (a) the EDSP's internal governance for the safeguard of the LC's Regulatory Records, and may be assessed by a number of criteria (such as the physical security of the storage facilities, and security over the network structures), and (b) subcontracting arrangement by the EDSP for data storage.

2. Maintenance of effective governance process with respect to the acquisition, deployment, and use of relevant software applications or services and ensuring the security, authenticity, reliability, integrity, confidentiality, and timely availability of information relating to the LC's business operations and client data (Relevant Information).

3. Implementation of a comprehensive information security policy to prevent any unauthorized disclosure. When information is encrypted, the LC must implement proper key management controls, maintain possession of the encryption and decryption keys, and ensure the keys are accessible to the SFC on demand without undue delay.

4. Implementation of appropriate policies, procedures, and controls to manage user access rights to ensure that Relevant Information can only be altered for proper purposes by authorized personnel, and is otherwise free from damaging and tampering.

5. LCs that use EDSP services, especially the public cloud, need to be aware of how the operation of these services and their exposure to cyber threats, in particular with regard to information confidentiality, integrity, and recoverability and the implementation of information and security controls.

6. Having a contingency plan.

7. Having in place an exit strategy to ensure that the external data storage or processing services can be terminated without material disruption to the continuity of any operations critical to the conduct of regulated activities, including if the EDSP becomes insolvent. The exit strategy should clearly outline how a transition to an alternative storage solution would be executed and how the SFC's access to Regulatory Records will not be impaired.

8. Having a legally binding service agreement with the EDSP (which should provide for contractual termination, and which may include contractual provisions requiring the EDSP to assist in a transition to a new EDSP and where relevant, clearly delineate the ownership of the data and the intellectual property following termination of the contract). Given LCs are required to notify the SFC of any proposed transition arrangement at least 30 calendar days prior to any termination, expiration, novation, or assignment of the service agreement with the EDSP, LCs should therefore ensure there is a provision in the service agreement with EDSP that the EDSP gives LCs sufficient notice before the EDSP terminates, novates, or assigns the service agreement.

APPENDIX – COMPLIANCE CHECKLIST FOR THE CIRCULAR

This checklist sets out key questions to consider for LCs that keep Regulatory Records with EDSPs in order to comply with the Circular. It consists of two parts: Part I sets out the requirements which LCs that use EDSPs exclusively must comply with in order to make an application to the SFC. Part II expands on the requirements in Part E of the Circular, which is relevant to LCs that use EDSPs either exclusively or nonexclusively.

This checklist is by no means exhaustive and is not tailored to the individual circumstances of each of the LC. Unless otherwise specified, capitalized terms used herein shall have the same meanings as those defined in the Circular.

I. Questions to Be Considered by LCs That Rely on EDSPs Exclusively

General	
✓	Is the EDSP suitable and reliable, having regard to the EDSP's operational capabilities, technical expertise, and financial soundness? To analyse this, LCs will need to conduct due diligence on the EDSP, which is covered in Part II below.
✓	Are all of the Regulatory Records kept with an EDSP fully accessible upon demand by the SFC without undue delay? Can they be reproduced in a legible form from the Hong Kong premises of the LCs as approved under Section 130 of the SFO?[5]
✓	Are Regulatory Records kept in a manner that does not impair or result in undue delays to the SFC's effective access to the Regulatory Records when it discharges its functions or exercises its powers (taking into account all pertinent political and legal issues in any relevant jurisdiction)? If needed, we would suggest LCs to obtain a legal opinion from counsel in the relevant jurisdictions to ensure that there is nothing under the laws, rules, or regulations of the relevant jurisdictions that would prevent the SFC from accessing Regulatory Records.
Audit Trail	
✓	Can the LCs provide detailed audit trail information in a legible form regarding any access to the Regulatory Records (including read, write, and modify) stored by the LCs at the EDSP? Is the audit trail a complete record of any access by the LCs to Regulatory Records stored with the EDSP? The audit trail should include information on time stamp, affected file, type of event, user ID, and user location (such as IP address).
✓	How long is the audit trail information to be kept? Is such period not less than the period for which the LCs are required to keep the Regulatory Records?
✓	Is the access of the LCs to the audit trail information restricted to read-only?
✓	Can each user who has accessed Regulatory Records be uniquely identified from the audit trail?
EDSP MICs[6] LCs are required to designate at least two individuals who are EDSP MICs in Hong Kong. The following questions may need to be considered:	
✓	Do the EDSP MICs have the knowledge, expertise, and authority to access all of the Regulatory Records kept with an EDSP at any time?
✓	Are the EDSP MICs able to ensure that the SFC has effective access to such records upon demand without undue delay in the exercise of its statutory powers?
✓	Do the EDSP MICs, or their delegates, have in their possession all digital certificates, keys, passwords, and tokens to ensure full access to all Regulatory Records kept with the EDSP?
✓	Can the EDSP MICs or their delegates discharge the following responsibilities at all times? (i) Provide all necessary assistance to the SFC to secure and promptly gain access to all of the Regulatory Records of the firm kept at the EDSP; and (ii) Put in place all necessary policies, procedures, and internal controls to ensure that the SFC has full access to all Regulatory Records upon demand without undue delay.

[5] As noted in the implementation issues above, there are practical challenges around producing data, and the industry is working with the SFC on a possible solution.

[6] This is one of the most contentious topics in the Circular (see implementation issues above) and there is extensive dialogue between the SFC and the industry. We will keep readers updated.

✓	LCs should also submit the following information to the SFC[7]: In respect of each of their EDSP MICs, the following particulars: (a) full name (b) identification information (c) job title (d) place of residence (e) the core function(s) which he or she is in charge of (f) the job title(s) of the person(s) to whom he or she reports within the corporation and, if applicable, within their corporate group. In addition, LCs should submit an updated organisational chart depicting their management and governance structure, business, and operational units and key human resources and their respective reporting lines. The chart should capture all MICs engaged by the LCs, their respective reporting lines, and the job titles of the persons reporting directly to these EDSP MICs in relation to the operations of the LCs.
Approval of Premises	
✓	Have the LCs sought approval for the premises used for keeping Regulatory Records (including the principal place of business and branch offices) under Section 130 of the SFO (see the section below)?

Approval of Premises for Keeping Regulatory Records

Regarding the application for approval for premises used for keeping Regulatory Records under Section 130 of the SFO (as mentioned in the above section), LCs need to provide details of the premises—which should be the principal place of business—of the LCs in Hong Kong where all of their Regulatory Records that are kept with the EDSPs are fully accessible upon demand by the SFC without undue delay. LCs also need to provide details of each branch office of the LCs in Hong Kong where their Regulatory Records kept with the EDSPs can be accessed.

LCs must also comply with the following requirements:

In Case of an HK EDSP	
✓	LCs must provide a confirmation that the requirements in Paragraph 7(a) of the Circular are satisfied, i.e., the LCs' Regulatory Records that are kept exclusively with the EDSP will be kept at such data center at all times throughout the period in which the Regulatory Records are required to be kept by law or regulation.
✓	A copy of the Notice from the LCs to the EDSP, countersigned by the EDSP.
In Case of a Non-HK EDSP	
✓	A copy of the Notice from the LCs to the EDSP.
✓	The Undertaking by the EDSP.

[7] See SFC's Circular titled "Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management," dated December 16, 2016.

II. Questions to Be Considered by LCs Using External Data Storage or Processing Services in General

Part E of the Circular sets out the general obligations of LCs using external data storage or processing services, regardless of whether the LC uses EDSPs exclusively or nonexclusively. To ensure compliance with such obligations as well as any other obligations under SFC codes and guidelines, LCs may wish to consider the following questions. In preparing this checklist, we have referred to the ABS Cloud Computing Implementation Guide 2.0 for the Financial Industry in Singapore published by the Association of Banks in Singapore.

Governance	
✓	Have the LCs designed a governance framework, which covers at least the following areas: (i) governance body to oversee the EDSP (ii) due diligence framework of the EDSP (iii) procedures to oversee the EDSP's adherence to the contractual and service level agreements (iv) procedures to review key performance indicators and frequency of such reviews (v) procedures to oversee the EDSP's sub-contracting arrangements (vi) assessment of the EDSP's cybersecurity framework, controls to protect data confidentiality and integrity, and locations where the data will be hosted (vii)management and escalation of security incidents (viii) contingency and business continuity plans; and (ix) exit plans LCs should adopt a risk-based approach in assessing the EDSP. LCs should seek input from the EDSP in designing and implementing the governance framework.
✓	In addition to the two EDSP MICs, who should be part of the governance body? Should a representative from the EDSP be part of the governance body? To whom should the governance body report?
✓	How often should the governance body meet?
✓	Do the LCs have governance process for (i) the acquisition, deployment, and use of software applications or services which read, write, or modify Relevant Information, and (ii) ensuring the security, authenticity, reliability, integrity, confidentiality, and timely availability of their Relevant Information?
Due Diligence	
✓	Have the LCs conducted due diligence on the financial strength and resources of the EDSP?
✓	Have the LCs conducted due diligence on the corporate governance framework of the EDSP?
✓	Are the LCs aware of the location of the data centers? It is important for LCs to ascertain and agree on which countries are acceptable for the LCs' Regulatory Records to be processed and reside to ensure the SFC has unfettered access to Regulatory Records?
✓	LCs should conduct due diligence on all of the data center locations that support processing and storage of LCs' data. Generally speaking, the EDSP or a qualified third party should have conducted assessments on all of their data centers in different locations. LCs should obtain a copy of such assessment. The assessment should at least include the data centers' perimeter, physical and environmental security, natural disasters, political and economic climate of the country where the data centers reside for the purposes of identifying any security and operational weaknesses. The EDSP should obtain periodic update on the assessment. The EDSP should also confirm the controls are consistent across all of their data centers in different locations.
✓	Have the LCs conducted due diligence over EDSP's policies and procedures relating to the

	safeguard of the LC's Regulatory Records?[8]
✓	Does each due diligence cover a subcontracting arrangement (if any) by the EDSP for the storage of the LCs' Regulatory Records, especially with regard to cyber risk management and information security?[9]
✓	When performing due diligence activities, are there appointed individuals and a central point to coordinate activities between the LCs and the EDSP?
Information Security Policy	
✓	Is the information security policy reasonably designed to prevent any unauthorized disclosure?
✓	Does this policy include an appropriate data classification framework, descriptions of the various data classification levels, a list of roles and responsibilities for identifying the sensitivity of the data, and the corresponding control measures?
✓	What are the steps the LCs will take to ensure the EDSP protects confidential Relevant Information from being intentionally or inadvertently disclosed to, or misused by, unauthorized third parties?
✓	What are the procedures and mechanisms to safeguard the confidentiality and security of the LCs' confidential Relevant Information? For example, do the LCs encrypt it while at rest and in transit? When it is encrypted, do the LCs implement any key management controls, or maintain possession of the encryption and decryption keys? Are the keys accessible to the SFC on demand without undue delay where any electronic record is required to be produced in the exercise of its statutory powers?[10]
✓	Will the LCs review and monitor the security practice of the EDSP on a regular basis (e.g., by appointing auditors or experts) to ensure the security of the LCs' Regulatory Records?
✓	What are the procedures the LCs will put in place to ensure any breaches or serious incidents that may impact the LC's data confidentiality and personal data information are promptly disclosed?
Access Rights Control	
✓	Have the LCs implemented policies, procedures, and controls to manage user access rights? Are LCs able to ensure that Relevant Information can only be altered for proper purposes by authorized personnel, and is otherwise free from damage or tampering?
Where LCs Are Keeping Only Part of Their Relevant Information with the EDSP	
✓	Are there controls put in place to prevent the migration of Relevant Information to the EDSP without proper authorization?
For LCs Using EDSP Services, Especially the Public Cloud	
✓	How is the allocation of responsibilities (e.g., the configuration of security settings, workload protection and credential management) between the LCs and the EDSP defined? Is such allocation clearly understood and properly managed by the LCs?

[8] This may include assessing the physical security of the storage facilities, the type of hosting (i.e., whether it is dedicated or shared hardware), security over the network infrastructure, IT systems and applications, identity and access management, cyber risk management, information security, data loss and breach notifications, forensics capabilities, disaster recovery, and business continuity processes.

[9] Regarding the contractual provisions with respect to subcontracting, please refer to the questions relating to the service agreement with the EDSP below.

[10] As noted under the implementation issues relating to two EDSP MICs above, for global financial institutions, it may not be possible for the two EDSP MICs based in Hong Kong or their delegates to maintain possession of the encryption and decryption keys. This is currently being discussed with the SFC.

✓	Shall the LCs use security automation as well as the security services and tools offered by the EDSP, in order to maintain a consistent level of security? Should such services or tools use encryption, the LCs must maintain possession of the encryption and decryption keys.[11]
Where LCs Are Using Other Forms of Virtual Storage	
✓	What are the control measures being implemented? Are they appropriate having regard to the increased complexity and security risk as compared to a non-virtual environment?
For LCs Using External Data Storage or Processing Services in the Conduct of Their Regulated Activities	
✓	What is the level of their dependence on the prompt and consistent delivery of services by their service provider?
✓	What is the potential operational impact on the LCs and their clients if the services are disrupted?
✓	Are there any appropriate contingency plans to ensure the LCs' operational resilience, and to require the EDSP to disclose data losses, security breaches, or operational failures, which may have a material impact on the LCs' regulated activities?
✓	Have the LCs determined the EDSP has a satisfactory business continuity plan? Prior to contracting with the EDSP, the LCs should verify the EDSP's ability to resume business within a mutually agreed targeted duration of time after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
✓	Have the LCs proactively sought assurance on the state of the EDSP's business continuity plan? Have the LCs considered participation in joint testing of the business continuity plan if possible?
Exit Strategy	
✓	Is there any exit strategy in place?
✓	Does the exit strategy take into account different considerations, such as (i) agreed procedures and tools to be used for deletion of data in a manner that data is rendered irrecoverable; (ii) removal of all LCs' data and confirmation that all data has been rendered irrecoverable on termination of the service agreement with the EDSP; and (iii) transferability of the external data storage or processing service (e.g., to another EDSP or back to the LCs) for the purpose of continuity of service?
✓	Can such strategy ensure that the external data storage or processing services can be terminated without material disruption to the continuity of any operations critical to the conduct of regulated activities by the LCs, including in the case of the insolvency of the service provider?
✓	***If Regulatory Records are stored exclusively with an EDSP –*** (i) how would a transition to an alternative storage solution be executed; and (ii) how would the SFC's access to Regulatory Records pursuant to the exercise of its regulatory powers not be impaired during the transition?
✓	How often is the exit strategy reviewed or updated?
Service Agreement with EDSP	
✓	Is there a legally binding service agreement with the EDSP, which provides for contractual termination?
✓	Does such agreement at least cover the following areas? (i) include contractual provisions requiring the EDSP to assist in a transition to a new EDSP or allow a migration of data back to storage at the premises of the LCs? (ii) where relevant, clearly delineate the ownership of the data and intellectual property following termination of the contract? (iii) set out all terms and conditions governing the roles, relationships, obligations, and responsibilities of all contracting parties? (iv) reflect the contracting parties' expectations on different aspects (e.g., technology risk

[11] Please see footnote 10.

	management and business continuity management), so that the LCs can be assured that there is stringent governance on the EDSP's daily operational procedures? (v) require the EDSP to give LCs sufficient notice before the EDSP terminates, novates, or assigns the service agreement as the LCs are required to give the SFC 30 calendar days advance notice? (vi) address the issue of the party liable for losses in the event of breach of security or confidentiality and the EDSP's obligation to the LCs? (vii) provide LCs with a right to review and monitor the security practices and control processes of the EDSP on a regular basis (and if needed, to appoint an expert or arrange for an auditor or qualified experts to provide a report) (viii) include situations where LCs may elect to terminate the agreement (for example, change of control, insolvency, serious breach of security or confidentiality or where there is a demonstrable deterioration in the ability of the EDSP to perform the service?
✓	***Subcontracting –*** Does such agreement: (i) enable the LCs to retain the ability to monitor and control the agreement when an EDSP uses a subcontractor to support material services? (ii) provide for an appropriate notification method between the LCs and the EDSP for changes in material subcontracting of the agreement? (iii) provide that the EDSP remains accountable to the LCs for the subcontractor's performance and the EDSP will remediate any failure to perform by the subcontractor? (iv) provide that the EDSP is liable for the performance and risk management of the subcontractor?
Protection Against Concentration Risk	
✓	Having regard to the scale of the LCs' operations and the extent of their use of data storage or processing by an EDSP, shall the LCs use more than one EDSP, or put in place alternative arrangements?

Contact

If you have any questions or would like more information on the issues discussed in this White Paper, please contact the following Morgan Lewis lawyer:

Hong Kong
Helen Fok +852.3551.8565 helen.fok@morganlewis.com

About Us

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.