CHARLTONS

SOLICITORS

Hong Kong December 2019

SFC Circular on Licensed Corporations' Use of External Electronic Data Storage

I. Licensed Corporations' Compliance with Statutory Record-Keeping Obligations

On 31 October 2019, the Securities and Futures Commission (**SFC**) issued a circular to licensed corporations on the use of external electronic data storage[1] (the **Circular**) aimed at giving licensed corporations more flexibility in how they comply with their statutory record-keeping obligations under the Securities and Futures Ordinance (**SFO**) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (**AMLO**). The various records and documents required to be maintained are referred to as "Regulatory Records".

Licensed corporations are required to ensure the preservation and integrity of Regulatory Records as well as their authenticity, reliability and accessibility if they are required to be produced in legal proceedings initiated by the SFC or the Department of Justice. Section 130 SFO further requires licensed corporations to obtain prior written consent from the SFC for any premises they use for keeping Regulatory Records related to the regulated activity/ies for which they are licensed.

The Circular notes that licensed corporations must comply with the statutory requirements for the keeping of records when they use external electronic data storage providers (**EDSPs**) for keeping Regulatory Records. Examples of the statutory obligations include, without limitation, those under:

i) the Securities and Futures (Keeping of Records) Rules[2] (Cap. 571O);

ii) Paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the SFC; and

iii) the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the SFC, particularly Section IV on 'Information Management'.

The Circular explains the approval requirements where licensed corporations keep Regulatory Records with EDSPs rather than at premises approved under section 130 SFO and sets out the requirements that apply where records are stored with EDSPs and the regulatory standards that apply when information is kept or processed electronically using EDSPs.

II. Scope of the Circular on Licensed Corporations' Use of External Electronic Data Storage

For the purpose of the Circular, External Data Storage Providers include external providers of:

a) public and private cloud services;

b) servers or devices for data storage at conventional data centres;

c) other forms of virtual storage of electronic information; and

1 SFC. "Circular to Licensed Corporations – Use of external electronic data storage". 31 October 2019. At: https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59

2 https://www.elegislation.gov.hk/hk/cap571O

d) technology services whereby (i) information is generated in the course of using the services, and the information is stored at such technology service providers or other data storage providers, and (ii) the information generated and stored can be retrieved by such technology service providers.

However, the requirements of the Circular's sections C and D (for keeping Regulatory Records exclusively with an EDSP and for approval of premises for keeping Regulatory Records) do not apply to:

a) a licensed corporation which keeps Regulatory Records with an EDSP if it contemporaneously keeps a full set of identical Regulatory Records at premises used by the licensed corporation in Hong Kong which has been approved under section 130 SFO (e.g. when cloud storage is used for the purposes of data backup); or

b) a licensed corporation which uses computing services without keeping Regulatory Records with an EDSP (e.g. where cloud computing services are only used for computations and analytics while Regulatory Records are kept at the licensed corporation's premises).

III. Requirements for Regulatory Records Kept Exclusively with an External Data Storage Provider

If a licensed corporation keeps its Regulatory Records exclusively with an EDSP, meaning it does not contemporaneously keep its Regulatory Records at premises used by the licensed corporation in Hong Kong, the Circular requires that:

a) the EDSP should either be incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance. In addition, it should be staffed by personnel operating at a data centre located in Hong Kong (**Hong Kong EDSP**) and the licensed corporation's Regulatory Records must be kept at that centre;

b) alternatively, if the EDSP is not a Hong Kong EDSP, the licensed corporation must obtain an undertaking by the EDSP, substantially in the form of the template in Appendix 1[3] to the Circular, to provide assistance and Regulatory Records upon request by the SFC;

c) the licensed corporation should ensure that the EDSP is suitable and reliable, having regard to its operational capabilities, technical expertise and financial soundness;

d) the licensed corporation should ensure that all its Regulatory Records can be accessed promptly and in full upon request by the SFC, and can be reproduced in a legible form from the licensed corporation's approved Hong Kong premises;

e) the licensed corporation must also ensure that:

i) it can provide detailed and complete audit trail information in a legible form regarding any access, including access by the licensed corporation, to the Regulatory Records (including read, write and modify) stored by the licensed corporation at the EDSP;

ii) the audit trail information is kept for the period for which Regulatory Records are required to be kept;

iii) the licensed corporation's access to the audit trail information should be restricted to read-only; and

iv) each user who has accessed the Regulatory Records can be uniquely identified from the audit trail;

f) the licensed corporation must ensure that Regulatory Records are kept in a manner that does not impair or result in undue delays to the SFC's effective access to the Regulatory Records, taking into account all relevant political and legal issues in any relevant jurisdiction. This requirement applies irrespective of where the EDSP maintains its hardware for the storage of information; and

3 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/openAppendix?refNo=19EC59&appendix=0

g) licensed corporations are also required to designate at least two individuals, being the Managers-In-Charge of Core Functions (**MICs**) in Hong Kong, who (i) have the knowledge, expertise and authority (including all necessary digital certificates, keys, passwords and tokens) to access all Regulatory Records kept with the EDSP, and (ii) can ensure that the SFC has effective access to such records upon demand without undue delay.

   The MICs will be responsible for:

   i) ensuring information security to prevent unauthorised access, tampering or destruction of Regulatory Records;

   ii) providing all necessary assistance to the SFC to secure and promptly gain access to all the Regulatory Records of the firm kept at the EDSP, and

   iii) putting 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. The licensed corporation and the designated MICs should also ensure that the above responsibilities of the designated MICs can and will be discharged at all times; and

h) the licensed corporation must seek approval for the premises used for keeping Regulatory Records under section 130 of the SFO.

IV. SFC Approval of Premises for Keeping Regulatory Records

Before keeping any Regulatory Records exclusively with an EDSP, a licensed corporation must:

a) apply for approval for the data centre(s) used by the EDSP at which the licensed corporation's Regulatory Records will be kept;

b) provide details of the premises, being the principal place of business, of the licensed corporation in Hong Kong where all of its Regulatory Records which are kept with the EDSP are fully accessible upon demand by the SFC without undue delay; and

c) provide details of each branch office of the licensed corporation in Hong Kong where its Regulatory Records kept with the EDSP can be accessed.

Both the principal place of business and the branch office(s) referred to in (b) and (c) above are required to be premises which the SFC has approved under section 130 SFO.

To apply for approval, the licensed corporation should submit an application together with:

a) where it is a Hong Kong EDSP and the Regulatory Records are kept there at all times:

   i) a confirmation to that effect from the licensed corporation (**Confirmation**); and

   ii) a copy of a notice from the licensed corporation to the EDSP (**Notice**), substantially in the form of the template in Appendix 2[4] to the Circular, authorising and requesting the EDSP to provide the licensed corporation's records to the SFC, countersigned by the EDSP as evidence of the EDSP's recognition of such authorization and request (**Countersignature**); and

b) where it is not a Hong Kong EDSP:

   i) a copy of the Notice from the licensed corporation to the EDSP, and

   ii) the undertaking by the EDSP to provide assistance and Regulatory Records upon request by the SFC substantially in the form of Appendix 2 to the Circular.

The SFC may approval grant approval subject to any conditions it considers reasonable in the circumstances. The licensed corporation should notify the EDSP and the SFC of the proposed transition arrangement at least 30 calendar days prior to any termination, expiration, novation or assignment of the service agreement with the EDSP.

V. General Obligations of Licensed Corporations Using External Data Storage or Processing Services

4 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/openAppendix?refNo=19EC59&appendix=2

Licensed corporations are under an obligation under the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the SFC to (i) have effective policies and procedures to properly manage risks to which the firm and its clients are exposed in relation to client data and information relevant to the firm's business operations (**Relevant Information**), and (ii) to implement information management controls to detect and prevent unauthorised access, insertion, alteration or deletion of Relevant Information.

The Circular requires licensed corporations using external data storage or processing services to implement the following control measures to properly manage cyber and operational risks, regardless of whether Regulatory Records are kept exclusively with an EDSP:

a) Licensed corporations should conduct initial due diligence on the EDSP and its controls relating to its infrastructure, personnel and processes for delivering data storage service and regularly monitor its service delivery. This due diligence should cover:

   i) any subcontracting arrangement by the EDSP for the storage of the licensed corporation's Regulatory Records, especially with regard to cyber risks and information security; and

   ii) the EDSP's internal governance for safeguarding the licensed corporation's Regulatory Records kept with the EDSP which may include assessing (1) the physical security of the storage facilities, (2) the type of hosting (dedicated or shared hardware), (3) security over the network infrastructure, (4) IT systems and applications, (5) identity and access management, (6) cyber risk management, (7) information security, (8) data loss and breach notifications, (9) forensics capabilities, (10) disaster recovery and (11) business continuity processes.

b) The licensed corporation should maintain an effective 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 its Relevant Information as appropriate.

c) The licensed corporation should implement an information security policy to prevent unauthorised disclosure, which should include: (i) a data classification framework, (ii) descriptions of various data classification levels, (iii) a list of roles and responsibilities for identifying the sensitivity of the data and the corresponding control measures; (iv) appropriate steps to ensure that the EDSP protects the confidentiality of Relevant Information; (v) procedures to safeguard the confidentiality and security of the Relevant Information by proper encryption management, and (vi) implement proper key management controls, maintain possession of encryption and decryption keys and ensure that the keys are accessible to the SFC on demand.

d) The licensed corporation should ensure that Relevant Information can only be altered for proper purposes by authorised personnel, and that each user who has accessed Regulatory Records can be uniquely identified; It should also ensure that any migration of Relevant Information is properly authorised.

e) The licensed corporation should ensure that the allocation of responsibilities, such as the configuration of security settings, workload protection and credential management, between the licensed corporation and the EDSP is well-defined, clearly understood and properly managed by the licensed corporation. It should be aware of how the operation of these services and their exposure to cyber threats may differ from a computing environment at the premises of the licensed corporation. Where the licensed corporation uses encryption, it should also comply with the requirements set out in sub-paragraph (c) above.

f) Given the increased complexity and security risk as compared to a non-virtual environment, licensed corporations using other forms of virtual storage should implement appropriate control measures; licensed corporations using external data storage in the conduct of its regulated activities should establish appropriate contingency plans to ensure its operational resilience, and require the EDSP to disclose data losses, security breaches, or operational failures.

g) The licensed corporation should have in place an exit strategy to ensure that the external data storage can be terminated without material disruption to the continuity of any operations critical to the conduct of regulated activities; if Regulatory Records are stored exclusively with an EDSP, it should outline how an alternative storage solution would be executed while the SFC's access to Regulated Records would not be affected during the transition period. In both cases, the exit strategy should be regularly reviewed and updated as appropriate.

h) The licensed corporation should have a legally binding service agreement with the EDSP setting out provisions in relation to contractual termination, such as requiring the EDSP to assist in the transition to a new EDSP, allowing a migration of data back to storage at the premises of the licensed corporation, and delineating the ownership of the data and intellectual property following termination of the contract.

i) The SFC notes that significant disruption to a major EDSP would impact the whole market and that depending on the scale of a licensed corporation's operations and the extent of its use of data storage or processing by an EDSP, a licensed corporation should consider whether it would be appropriate to use more than one EDSP, or to put in place alternative arrangements to ensure operational resilience.

VI. Compliance with Section 130 of the SFO

Licensed corporations using external electronic data storage are expected to comply with the requirements set out in s. 130 of the SFO, which requires prior written approval from the SFC to be obtained before using any premises for keeping records or documents.

Where any licensed corporation's Regulatory Records are kept exclusively with an EDSP before 31 October 2019, the licensed corporation should:

a) without undue delay, notify the SFC's Licensing Department of the Intermediaries Division; and

b) apply for approval under s. 130 of the SFO.

If any data centre of an EDSP used by the licensed corporation for exclusively keeping Regulatory Records has already been approved under s. 130 of the SFO before 31 October 2019, the licensed corporation should provide the SFC's Licensing Department with:

- the names of the two MICs and a confirmation that all Regulatory Records are fully accessible upon demand by the SFC in future events, without undue delay; and

- no later than 30 June 2020, the Confirmation, a copy of the Notice and the Countersignature, together with a confirmation that the Circular's other requirements have been complied with.

CHARLTONS

Boutique Transactional Law Firm of the Year 2017
Asian Legal Business Awards

Hong Kong Office
Dominion Centre
12th Floor
43-59 Queen's Road East
Hong Kong
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596

www.charltonslaw.com