SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

31 October 2019

Circular to Licensed Corporations

Use of external electronic data storage

1. The Securities and Futures Commission (**SFC**) has observed that the use of external electronic data storage, including public and private cloud storage, has become increasingly prevalent. Financial institutions utilise these storage services as they offer benefits such as scalability, availability and cost savings.

A. Introduction

2. Licensed corporations have to ensure the preservation and integrity of the records or documents they are required to keep under the Securities and Futures Ordinance (Cap 571) (**SFO**) or the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap 615) (**Regulatory Records**).

3. Under section 130 of the SFO, a licensed corporation shall not, without the SFC's prior written approval, use any premises for keeping records or documents relating to the carrying on of the regulated activity for which it is licensed. When using external electronic data storage providers (**EDSPs**) for keeping Regulatory Records, licensed corporations should remain in full compliance with the existing regulatory requirements[1]. Licensed corporations should ensure that the SFC's access to Regulatory Records, in a legible form[2], pursuant to the exercise of its regulatory powers[3] is not restricted or otherwise undermined, and that these Regulatory Records have not been deleted or tampered with. The authenticity[4], integrity and reliability of Regulatory Records, as well as the ability to access them promptly, are paramount if such records are required to be produced in legal proceedings initiated by the SFC or the Department of Justice.

4. To provide licensed corporations with greater flexibility in keeping Regulatory Records, as well as to clarify their general obligations in relation to electronic data, this circular:

   (a) sets out the requirements where licensed corporations' Regulatory Records are kept with EDSPs instead of at other premises approved under section 130 of the SFO, and explains the approval requirements for such record keeping;

   (b) explains the regulatory standards to be observed by licensed corporations when information is kept or processed electronically using EDSPs.

[1] Such as the Securities and Futures (Keeping of Records) Rules (Cap 571O), General Principle 3 and paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, and the Management, Supervision and Internal Control Guidelines For Persons Licensed by or Registered with the Securities and Futures Commission, in particular Section IV on "Information Management".
[2] Section 189 of the SFO.
[3] For instance, the SFC has powers under Part VIII of the SFO to require the production of any record or document containing information relevant to an investigation, or to require the production of any record or document from any person on premises specified in a warrant and who is reasonably believed to be employed in connection with a business conducted on the premises.
[4] This refers to the authenticity of the record itself (such as evidence demonstrating that a record was created at the time stated), rather than the authenticity of any information contained in the record.

B. Scope of this circular[5]

5. For the purposes of this circular, EDSPs[6] 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

   (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[7].

6. The requirements in sections C and D of this circular do not apply to:

   (a) a licensed corporation which keeps Regulatory Records with an EDSP if the licensed corporation contemporaneously also keeps a full set of identical Regulatory Records at premises used by the licensed corporation in Hong Kong approved under section 130 of the SFO, for example when cloud storage is only used for the purposes of data backup or ensuring data availability; or

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

C. Requirements for keeping Regulatory Records exclusively with an EDSP

7. A licensed corporation should ensure compliance with the following requirements if it wishes to keep any Regulatory Records exclusively[8] with an EDSP:

   (a) The EDSP (i) is either a company incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance (Cap 622)[9], in each case staffed by personnel operating in Hong Kong, and (ii) provides data storage to the licensed corporation at a data centre located in Hong Kong (**Hong Kong EDSP**). In addition, the licensed corporation's Regulatory Records which are kept exclusively with the EDSP will be kept at such data centre at all times throughout the period in which the Regulatory Records are required to be kept by law or regulation[10].

   (b) As an alternative, if the EDSP is not a Hong Kong EDSP as defined in paragraph 7(a), the licensed corporation must obtain an undertaking by the EDSP, substantially in the form of the template in Appendix 1 (**Undertaking**) of this

[5] This circular does not apply to the storage of physical Regulatory Records, or electronic copies of physical Regulatory Records when the physical Regulatory Records are being kept at premises in Hong Kong approved under section 130 of the SFO.
[6] EDSPs do not include agents which only perform a marketing or customer service function and do not keep or have access to any Regulatory Record of licensed corporations.
[7] A licensed corporation should only engage technology service providers that can retrieve the information generated and stored if it intends to keep Regulatory Records exclusively with such technology service providers.
[8] That is, where the licensed corporation does not contemporaneously keep a full set of identical Regulatory Records at premises used by the licensed corporation in Hong Kong approved under section 130 of the SFO.
[9] See Part 16 of the Companies Ordinance (Cap 622), in particular sections 776 and 777.
[10] This does not prevent the licensed corporation from maintaining an identical set of Regulatory Records outside Hong Kong.

circular, to provide Regulatory Records and assistance as may be requested by the SFC.

(c) A licensed corporation should only keep Regulatory Records with an EDSP which is suitable and reliable, having regard to the EDSP's operational capabilities, technical expertise and financial soundness.

(d) The licensed corporation should ensure that all of its Regulatory Records which are kept exclusively with an EDSP are fully accessible upon demand by the SFC without undue delay, and can be reproduced in a legible form from premises of the licensed corporation in Hong Kong approved for this purpose by the SFC under section 130 of the SFO.

(e) The licensed corporation should ensure that (i) it can provide detailed audit trail information[11] in a legible form regarding any access to the Regulatory Records (including read, write and modify) stored by the licensed corporation at the EDSP, and (ii) the audit trail is a complete record of any access by the licensed corporation to Regulatory Records stored by the EDSP. The audit trail information should be kept for the period for which the licensed corporation is required to keep the Regulatory Records. The access of the licensed corporation to the audit trail information should be restricted to read-only. The licensed corporation should ensure that each user who has accessed Regulatory Records can be uniquely identified from the audit trail.

(f) The licensed corporation should ensure that, irrespective of which EDSP is being used, and of where the EDSP maintains its hardware for the storage of information, 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 when it discharges its functions or exercises its powers, taking into account all pertinent political and legal[12] issues in any relevant jurisdiction[13].

(g) The licensed corporation should designate at least two individuals, being Managers-In-Charge of Core Functions (**MICs**) in Hong Kong, who have the knowledge, expertise and authority to access all of the Regulatory Records kept with an EDSP at any time, and 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 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 MICs will be responsible for ensuring information security to prevent unauthorised access, tampering or destruction of Regulatory Records. The MICs, or their delegates, must 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 put in place all necessary policies, procedures and internal controls to ensure that the SFC has full access to all

[11] Audit trails or data access logs should include, at a minimum, information on timestamp, affected file, type of event, user ID and user location (such as IP address).
[12] Such as legal issues related to personal data protection. In particular, the licensed corporation should also ensure it complies with the Personal Data (Privacy) Ordinance (Cap 486) when storing or processing data at an EDSP.
[13] Such as whether the jurisdiction is a signatory to the International Organization of Securities Commissions Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information.

Regulatory Records upon demand without undue delay. The licensed corporation and the designated MICs should ensure that the above responsibilities of the designated MICs can and will be discharged at all times.

(h) The licensed corporation should seek approval for the premises used for keeping Regulatory Records under section 130 of the SFO. See Part D below.

D. Approval of premises for keeping Regulatory Records

8. Before keeping any Regulatory Records exclusively with an EDSP, a licensed corporation which fulfils all of the above requirements should:

(a) apply for approval under section 130 of the SFO for the data centre(s) used by the EDSP at which the Regulatory Records of the licensed corporation 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 should also be premises approved or to be approved under section 130 of the SFO.

A licensed corporation must satisfy the SFC that the premises are suitable for the purpose of keeping Regulatory Records.

9. The licensed corporation's application for approval under section 130 of the SFO should be accompanied by:

(a) where the requirements in paragraph 7(a) are satisfied:
  (i) a confirmation of the same by 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 as set out in Appendix 2 of this 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 authorisation and request (**Countersignature**); and

(b) where the requirements in paragraph 7(a) are not satisfied:
  (i) a copy of the Notice from the licensed corporation to the EDSP, and
  (ii) the Undertaking by the EDSP.

The approval may be given subject to conditions which the SFC considers reasonable in the circumstances[14].

10. The licensed corporation should notify 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. The licensed corporation should ensure that the EDSP gives it sufficient notice before the EDSP terminates, novates or assigns the service agreement in order that it could fulfil this requirement.

E. General obligations of licensed corporations using external data storage or processing services

11. Licensed corporations are reminded of their obligations under the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (a) to have effective policies and procedures for the proper management of risks to which the firm and its clients are exposed with respect to client data and information relevant to the firm's business operations (**Relevant Information**), and (b) to implement information management controls to detect and prevent unauthorised access, insertion, alteration or deletion of Relevant Information. To properly manage cyber and other operational risks, a licensed corporation using external data storage or processing services should implement the following control measures in this section E, regardless of whether Regulatory Records are kept exclusively with an EDSP.

12. The licensed corporation should conduct proper initial due diligence on the EDSP and its controls relating to its infrastructure, personnel and processes for delivering its data storage services, as well as regular monitoring of the EDSP's service delivery, in each case commensurate with the criticality, materiality, scale and scope of the EDSP's service. Such due diligence should cover:

    (a) the EDSP's internal governance for the safeguard of the licensed corporation's Regulatory Records (where Regulatory Records are kept with the EDSP), and may include assessing the physical security of the storage facilities, the type of hosting (ie, 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; and

    (b) any subcontracting arrangement by the EDSP for the storage of the licensed corporation's Regulatory Records, especially with regard to cyber risk management and information security.

13. The licensed corporation should maintain an effective governance process for (a) the acquisition, deployment and use of software applications or services which read, write or modify Relevant Information, and (b) ensuring the security, authenticity, reliability, integrity, confidentiality and timely availability of its Relevant Information as appropriate.

[14] Section 403 of the SFO.

14. The licensed corporation should implement a comprehensive information security policy to prevent any unauthorised disclosure. This policy should 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. The licensed corporation should also take appropriate steps to ensure that the EDSP protects Relevant Information which is confidential from being intentionally or inadvertently disclosed to, or misused by, unauthorised third parties. To protect its confidential Relevant Information, the licensed corporation should encrypt it while at rest and in transit, or establish effective procedures and mechanisms to safeguard its confidentiality and security. When it is encrypted, the licensed corporation must implement proper key management controls, maintain possession of the encryption and decryption keys and ensure that the keys are 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.

15. The licensed corporation should implement appropriate policies, procedures and controls to manage user access rights to ensure that Relevant Information can only be altered for proper purposes by authorised personnel, and is otherwise free from damage or tampering. The sharing of system authentication codes (such as passwords) among users should generally be prohibited, with a view to ensuring that each user who has accessed Regulatory Records can be uniquely identified.

16. Where a licensed corporation is keeping only part of its Relevant Information with the EDSP (whether due to data sensitivity concerns or otherwise), it should put in place controls to prevent the migration of Relevant Information to the EDSP without proper authorisation.

17. Licensed corporations using EDSP services, especially the public cloud, need to 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, in particular with regard to information confidentiality, integrity and recoverability, and the implementation of information and security controls. Public cloud providers and users typically share responsibility for the security and control of the technology, and this may be more complicated than a traditional outsourcing model. Regardless of how the technology is deployed, 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. Additionally, the licensed corporation may consider using security automation as well as the security services and tools offered by the EDSP to maintain a consistent level of security. Should such services or tools use encryption, the licensed corporation must maintain possession of the encryption and decryption keys as specified under paragraph 14 above.

18. A licensed corporation using other forms of virtual storage should implement control measures which are appropriate for the increased complexity and security risk as compared to a non-virtual environment.

19. A licensed corporation using external data storage or processing services in the conduct of its regulated activities should assess the level of its dependence on the prompt and consistent delivery of services by its service providers as well as the potential operational

impact on the licensed corporation and its clients if the services are disrupted. The licensed corporation should establish appropriate contingency plans to ensure its operational resilience, and to require the EDSP to disclose data losses, security breaches, or operational failures which may have a material impact on the licensed corporation's regulated activities.

20. A licensed corporation should have 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 in the case of the insolvency of the service provider. If Regulatory Records are stored exclusively with an EDSP, this strategy should clearly outline how a transition to an alternative storage solution (which might include another EDSP) would be executed, and how the SFC's access to Regulatory Records pursuant to the exercise of its regulatory powers will not be impaired during the transition. The exit strategy should be regularly reviewed and updated as appropriate.

21. The licensed corporation should have a legally binding service agreement with the EDSP, which should provide for contractual termination. This may 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 licensed corporation and, where relevant, clearly delineate the ownership of the data and intellectual property following termination of the contract.

22. Concentration risk may arise where a major EDSP provides data services to a large number of financial firms, since a significant disruption in its services may have an impact on the market. Depending on the scale of a licensed corporation's operations and the extent of its use of data storage or processing by an EDSP, the licensed corporation should consider whether it is appropriate to use more than one EDSP, or put in place alternative arrangements to ensure operational resilience.

F. Compliance with section 130 of the SFO

23. Licensed corporations are expected to review their use of external electronic data storage to ensure compliance with section 130 of the SFO (including making an application for approval described in paragraph 8 above) and the regulatory expectations set out in this circular.

24. Where any licensed corporation's Regulatory Records are kept exclusively with an EDSP before the date of this circular, the licensed corporation should:

    - without undue delay, notify the SFC's Licensing Department of the Intermediaries Division; and
    - apply for approval under section 130 of the SFO.

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

    - without undue delay, the names of the two MICs as mentioned in paragraph 7(g) and a confirmation that all Regulatory Records of the licensed corporation which are kept

with the EDSP are fully accessible at the licensed corporation's principal place of business upon demand by the SFC;

- no later than 30 June 2020, the Confirmation, a copy of the Notice and the Countersignature, as required under paragraph 9(a), together with a confirmation that the other requirements in this circular have been complied with.

Should you have any queries regarding the contents of this circular, please contact Ms Coolky Sit at 2231 1767.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

Enclosure

End

SFO/IS/048/2019