AIMA APAC Webinar: A Conversation Between SFC & AIMA

10 December 2019

Speakers:

Kenneth Lai, Director, Enforcement, SFC

Kher Sheng Lee, Managing Director, Co-Head of APAC and Deputy Global Head of Government Affairs, AIMA

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

AIMA APAC Webinar: Latest SFC Circular On External Electronic Data Storage Providers (EDSPs)

10 December 2019

Panellists:

James Tedman, Partner, ACA Aponix

Derek McGibney, Director, ACA Compliance Group

Mark Shipman, Partner, Clifford Chance

Stuart Sanders, Executive Director, Velocity Solutions

Moderator: Kher Sheng Lee, Managing Director, Co-Head of APAC and Deputy Global Head of Government Affairs, AIMA

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

SFC Circular to Licensed Corporations (LCs) on Use of External Electronic Data Storage – 31 October 2019 (Circular)

Section 130 of the SFO

- LC requires SFC's prior written approval to use any premises for keeping records or documents relating to the carrying on of the regulated activity for which it is licensed

Basics - External Electronic Data Storage Providers (EDSPs) and Regulatory Records

- What is an EDSP?
- Public and private cloud services
- Servers or devices for data storage at conventional data centres
- Other forms of virtual storage of electronic information
- Technology services (i) information is generated in the course of using the services, and 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

Regulatory Records and Company's Data

- Regulatory records - records or documents that are required by the LC to keep under the SFO or AMLO
- Company's data - any information, data record or document relating to the company

Requirements For LCs' Records Kept Exclusively With EDSPs

Exclusive vs Non-Exclusive

- Exclusive - where the LC 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

Due Diligence and Suitability

- Proper due diligence on EDSP
- Comprehensive information security policies and procedures
- Proper management of user access

Accessibility of Regulatory Records

- Records are fully accessible upon demand by the SFC without undue delay, taking into account all pertinent political and legal issues in any relevant jurisdiction
- *Without giving the LC any notification*
- Records 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

Requirements For LCs' Records Kept Exclusively With EDSPs

Audit Trail

LC must ensure that it can provide audit trail information. The audit trail information should be detailed and complete regarding any access to the regulatory records

Governance

At least two Managers-In-Charge of Core Functions *in Hong Kong*. Responsibilities include the following:

- Put in place all necessary policies, procedures and internal controls
- Ensure SFC has effective access to the regulatory records
- Ensure information security over relevant information
- Have access to all passwords, keys, tokens, digital certificates and prepare of contingency

- **What to do now?**

Case Study – Office 365

- Office 365 - now the defacto email solution for most investment managers with many using SharePoint, Teams, and OneDrive.

- Unstructured and blended data repositories – will include records for regulated activities, e.g. trade ideas, orders, confirms and client conversations, as well as other company and personal data.

- How would the LC/EDSP provide access to the SFC?
  - Would require a login account and search tools to see across all LC mailboxes and storage
  - How does LC/EDSP maintain required security standards, e.g., multi-factor authentication on log-ins, download policies, and IP address whitelisting?
  - Office365 audit logs are only retained for 90 days
  - Conflict with privacy regulations - disclosure of personal data to the SFC
  - If the LC procures Office365 via another service provider, who is the effective EDSP in that instance?

Examples of Technical Implementation Challenges

- Identifying relevant datasets and repositories
- Segregating in-scope and out-of-scope data
- Access to blended data repositories such as email/file storage may expose LC to conflicts with privacy regulations and/or security risks
  - Liability in event of breach caused by SFC's access to data?
  - Conflicting regulatory requirements? SFC vs GDPR?
- Access to encrypted data held at EDSP e.g.,
  - EDSP may be storage vendor with encryption keys held by LC
  - EDSP may have encryption keys that are never provided to clients
- Audit trail
  - Use of shared accounts
  - Meeting audit trail requirements with local copies of data taken for non-exclusivity purposes
- Multiple outsourcing levels. What happens when the service is managed by one technology vendor, but runs on a service provided by another vendor, e.g., a white-labelled CRM using Microsoft Dynamics as the underlying platform, or Office 365 managed by another managed service provider?
- Datacentre Locations.
  - Some cloud services providers may not provide details on the datacentre locations for security reasons.
  - Services like Office 365/AWS may multi-home in multiple geographical locations, and the specific locations may not be visible to the administrators.

Q&A

Contact

Kher Sheng Lee
AIMA
E: kslee@aima.org

Derek McGibney
ACA Compliance Group
E: derek.mcgibney@acacompliancegroup.com

Stuart Sanders
Velocity Solutions
E: Stuart.Sanders@velocity-solutions.com

James Tedman
ACA Aponix
E: jtedman@acaaponix.com

Mark Shipman
Clifford Chance
E: mark.shipman@cliffordchance.com

Appendix I
Approval requirements

- LC's with Regulatory Records are kept exclusively with an EDSP ***before*** the date of the Circular

- Notify SFC without undue delay
- If EDSP (data center) is already approved
  - Provide names of two MICs responsible for and with access to the keys, passwords and tokens to provide access to the data
  - A confirmation that records are fully accessible to the SFC at their place of business
  - By 30 June 2020, provide a confirmation of compliance, a copy of the notice of requirements to the service provider, and their countersignature or undertaking, for overseas data center
- If an EDSP is an exclusive holder of Regulatory Records, and has not before 1 November, obtained approval they are required to notify the SFC licensing department of that fact, and apply for approval under section 130.

- Premises approval (under section 130 of SFO)
- *Before* keeping records exclusively with an EDSP, the LC should:
- Apply for approval for the data centre(s) used by the EDSP where the regulatory records will be kept
- Provide details of the premises, being the principal place of business, of the LC in Hong Kong where all of its regulatory records kept with the EDSP and provide details of each branch office of the LC in Hong Kong where its regulatory records kept with the EDSP can be accessed.
- Relevant confirmation, notice, countersignature, undertaking (where applicable)

APPENDIX II

Section E of the Circular – General obligations of LCs' records kept with external data storage providers or processing services (regardless of whether Regulatory Records are kept exclusively with an EDSP)

- Obligations under the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission
- Proper due diligence on EDSP and its controls
- Effective governance
- Comprehensive information security policy
- Appropriate user access rights policies and procedures and controls
- When LC is keeping only part of its Relevant Information with the EDSP, there must be controls in place to prevent improper migration of Relevant Information.
- Cyber threats and other technology risk considerations
- Appropriate control measures for non-virtual environment
- Disruption/Continuity Programmes to ensure operational resilience
- Legally binding service agreement with the EDSP