SFC requirements of Licensed Corporations on the use of external electronic data storage EDSP – UPDATED DEADLINE

Impact of COVID 19 and what to think about now

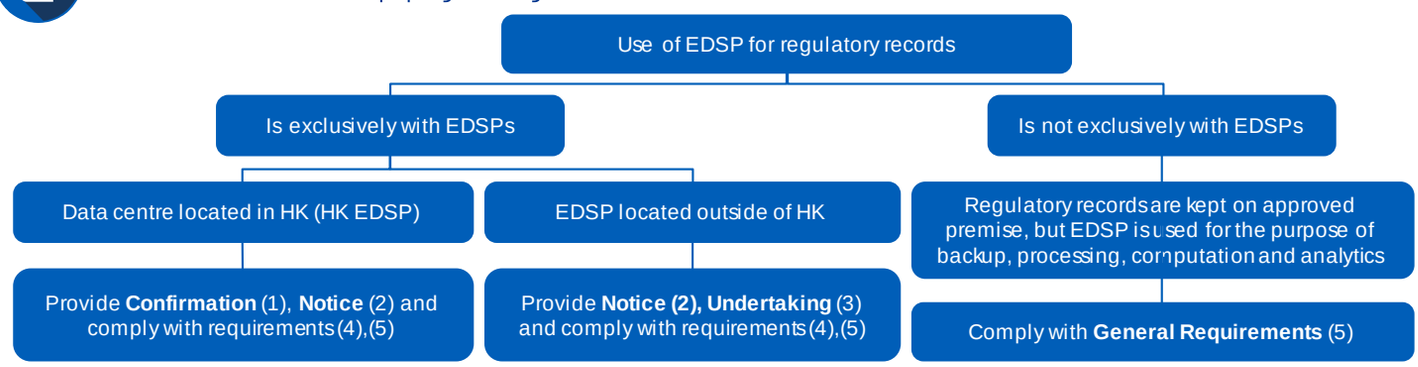
No one could have foreseen the global COVID-19 pandemic or the pace at which businesses have had to adapt to the '**new reality**'. **In reaction, LCs have had to quickly adapt to remote working and accelerating the rollout of digital tools and infrastructure**. The regulators have also reacted and the Securities and Futures Commission (SFC) has **extended** the deadline of the circular regarding external data storage providers (EDSPs) to **31 December 2020**.

We are just beginning to take stock of how we met the challenges we all faced. **Now is the time to see where we are on compliance with EDSP** to make sure that the safeguards and measures the regulator expects are in place. It is imperative that we **understand the impact of remote working and the adoption of digital tools** and, importantly, **where data is now stored**. This paper considers how to interpret the circular and how KPMG can help to quickly take stock of where you are and how to meet the new timeline.

Scope of the circular

1. Public and private cloud services
2. Servers or devices for data storage at conventional data centres
3. Other forms of virtual storage of electronic information
4. Technology services whereby
   a) information is generated in the course of using the services and is stored at such technology service providers or other data storage providers, and
   b) the information generated and stored can be retrieved by such technology service providers.

How does it apply to you?



(1) A confirmation from the LC that the EDSP is in fact a Hong Kong EDSP (**Confirmation**).
(2) A copy of the notice from the LC authorising and requesting the EDSP to provide the LC's records to the SFC (**Notice**), which has been countersigned by the EDSP (**Countersignature**).
(3) An undertaking to the LC to provide regulatory records and any assistance to the SFC as required (**Undertaking**).
(4) **Requirements for keeping regulatory records exclusively with an EDSP**

LCs which **exclusively rely on EDSPs** for the storage of regulatory records are required to fulfill a number of significant obligations, the key ones are shown below:

Designated managers-in-charge (MIC)
At least two MICs effectively responsible for overseeing the use of EDSPs.

Audit trail of access information
Able to provide a detailed, complete and legible audit trail of access to the regulatory records.

SFC's access to regulatory records
All regulatory records at the EDSP are fully accessible by the SFC without undue delay.

Ongoing notification to SFC
Notify the SFC at least 30 calendar days prior to any assignment, renewal, expiration or termination of the EDSP agreement.

(5) General requirements on use of external data storage

All LCs using external data storage or processing services are expected to execute the following control measures, **regardless of whether regulatory records are kept exclusively with EDSPs or not:**

Policies and procedures
Implement policies and procedures for proper risk and information management controls e.g. internal review and analysis.

Due diligence
Conduct initial and on-going due diligence on EDSP's service delivery, e.g. internal governance of safeguarding Regulatory Records.

Access to program and data
Ensure proper control on user access rights and effective governance processes are in place for the use of software, e.g. reading and modification rights.

Service agreement
Define a clear allocation of responsibilities and provision of services between LCs and EDSPs, e.g. termination and transitional plans.

Information and cyber security
Execute information and cyber security policy to protect against cyber threats and unauthorized use of regulatory records, e.g. use of encryption.

Exit strategy
Formulate an exit strategy to ensure no material disruption of the service termination on external data storage or processing, e.g. regular review on exit plan.

Key questions for LCs to consider

COVID response activities	1. Do you know how newly implemented tools or activities have impacted where your data is? 2. Do you have a clear log of all changes made and understand the impact on operations? 3. Do you have the expected documentation and approvals in place should the regulator ask?
Internal audit, risk & control	4. Are regulatory records fully accessible upon demand by the SFC without undue delay? 5. Do you have adequate safeguards on the regulatory records (e.g. Cloud Security Vault)? 6. Do you have sufficient data protection at rest and in transit (e.g. encryption, tokenisation, etc.)?
Information risk management	7. Is there a legible audit trail regarding any access to regulatory records? 8. Do you have effective policies, guidelines and controls in place for your EDSPs? 9. Does your EDSP have a subcontractor(s)? If yes, do they have effective controls in place?
Data governance and quality	10. Do you have the right governance in place to support data management processes? 11. Is there a formal data ownership model in place? 12. Do you trust the quality of the your regulatory data which will be accessed by the SFC?
Cloud security	13. What is your current cloud security maturity level? 14. Have you assessed the impact on your technology stack and data repositories?

How can KPMG help you?

Assessment & planning
- Summarise the requirements into practical actions.
- Build a plan, including timelines and reporting criteria.
- Assess any in-flight projects that can be leveraged.

Gap analysis & recommendations
- Conduct gap analysis against KPMG's external data storage governance framework.
- Provide recommendations on next steps to become compliant.

Implementation & review
- Build an end-to-end detailed plan of actions based on the recommendations.
- Help implement recommendations.
- Perform post-implementation review to ensure full compliance.

Our other relevant propositions to support you on this journey:

IT control assessments	Cloud security	Cloud migration
Risk and controls	Data governance and ownership	IT and data strategy

Contact us

James O'Callaghan
Partner, IT Advisory
KPMG China
T: +852 2143 8866
E: james.ocallaghan@kpmg.com

Tom Jenkins
Partner, Financial Risk Mgmt.
KPMG China
T: +852 2143 8570
E: tom.jenkins@kpmg.com

Jia Ning Song
Partner, Risk Consulting
KPMG China
T: +852 2978 8101
E: jianing.n.song@kpmg.com

Adam Stuckert
Partner, IT Advisory
KPMG China
T: +852 2522 6022
E: adam.stuckert@kpmg.com

Susanne Steyn
Director, Risk Consulting
KPMG China
T: +852 2140 2317
E: susanne.steyn@kpmg.com

Brian Cheung
Director, IT Advisory
KPMG China
T: +852 2522 6022
E: brian.cheung@kpmg.com

kpmg.com/cn