KPMG

符莎莉律師事務所
SF Lawyers
In association with KPMG Law

Implications of Cross-border Data Transfers for Hong Kong SAR-based Financial Institutions

Key considerations and challenges in China's evolving data protection regulations

September 2023

Stay Up-to-Date: Cross-border Data Transfer Regulations and Compliance

Hong Kong SAR-based businesses that collect and transfer information across borders are required to ensure they comply with new laws and guidelines related to privacy and data security. The Chinese Mainland is among the many jurisdictions that have implemented these regulations, which cover various scenarios and affect many financial institutions.

The complexity of the rules can pose challenges for many Hong Kong SAR-based organisations, so it is crucial that they fully understand the requirements and have protocols in place to manage cross-border data transfers.

This flyer serves as a reference point for Hong Kong SAR-based businesses affected by the rules to help ensure compliance. Stay informed about complex and constantly changing regulations regarding the handling of personal information and other data to avoid potential compliance issues.

Overview of Key Regulations

The Chinese Mainland is among the jurisdictions globally that has implemented new laws and guidelines related to privacy and data security in recent years. The new regimes and regulations present compliance considerations for organisations that collect and transfer information across borders. The major regulations are listed below:

Cybersecurity Law ("CSL")

June 1, 2017

Lists the restrictions on the transfer of personal information and business data overseas

Data Security Law ("DSL")

September 1, 2021

Emphasises the requirements for Cross-border Data Transfer ("CBDT") of Critical Infrastructure Operator ("CIIO") and important data

Personal Information Protection Law ("PIPL")

November 1, 2021

Provides guidance for cross-border data transfer of personal information

Measures for Cross-border Data Transfer Security Assessment

September 1, 2022

Specifies key review aspects to be covered in Cross-border Data Transfer Self-Assessment and Cyberspace Administration of China ("CAC") Security Assessment

Announcement on the Implementation of Personal Information Protection Certification

November 4, 2022

Lists the key standards for obtaining the personal information protection certification for personal information processors with cross-border data transfers

Measures for Standard Contracts for Cross-border Transfer of Personal Information

June 1, 2023

Provides guidance on the compliance path for data processors that will enter into a contract agreement with overseas data recipients

Measures for the Administration of Data Security in the Business Areas of the People's Bank of China (Draft for Comments)

July 18, 2023

Strengthen the requirements for storing data within China and compliance with the relevant CBDT regulations

Administrative Measures for the Compliance Audit of Personal Information Protection (Draft for Comments)

August 3, 2023

Puts forward guidelines for periodic audit reviews for personal information processing activities

Compliance Paths

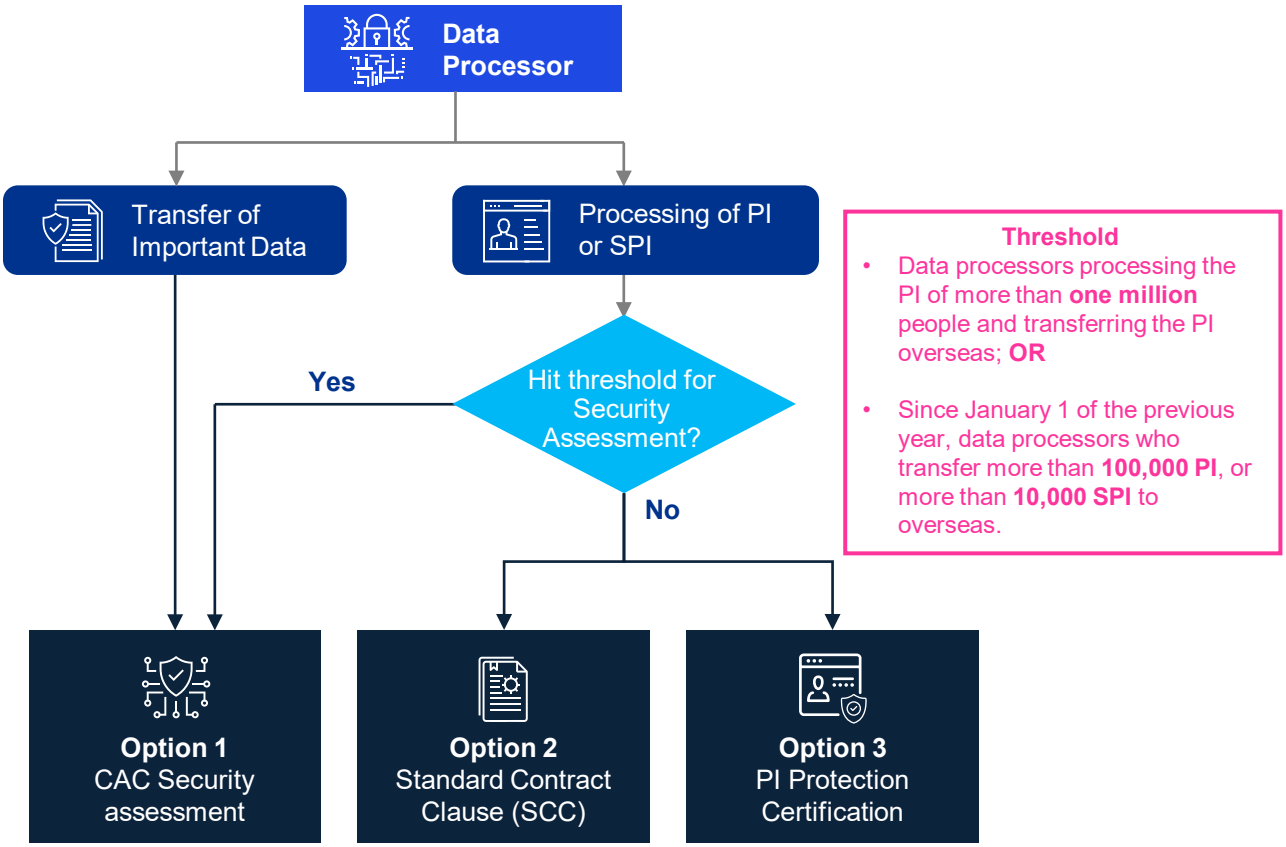
To assess the potential impact, organisations should consider the following regulatory information regarding cross-border data transfers:

Personal Information ("PI"): Information that pertains to either identified or identifiable natural persons.

Sensitive Personal Information ("SPI"): Personal information that if disclosed or used illegally, could result in harm to an individual's dignity, personal safety or property.

Important Data: Data that, once tampered, destroyed, leaked, illegally obtained or used, may pose threats to national security, economic operations, social stability, public health or security.

Three compliance paths have been outlined for organisations to adhere to when conducting cross-border data transfers, depending on the type of data being transferred. The graph below illustrates the options.



Cross-border Data Transfer Scenarios for Hong Kong SAR Financial Institutions

There are various scenarios that may be considered as cross-border data transfers. Some specific scenarios that a Hong Kong-based organisation may encounter include:

An organisation receives regulated data (i.e. including PI, SPI or important data) shared by its Chinese Mainland-based counterpart, such as through email, system, FTP, etc.

An organisation hosts its data centre and systems within Hong Kong and collects regulated data from the Chinese Mainland

An organisation hosts its data centre and systems within the Chinese Mainland, where it collects regulated data, and allows Hong Kong staff to remotely access the corresponding server or database for system maintenance

In the above scenarios, an organisation should assess and evaluate whether they are required to comply with the relevant cross-border data transfer requirements and determine the next actions.

Common Challenges

Managing data security and privacy requires a different approach than traditional information security. It involves integrating with business processing scenarios to address topics like legal compliance and technical protection. This demands a higher level of internal cooperation within enterprises. Many organisations in Hong Kong are facing challenges, in areas including:

Not having clear guidelines or protocols for managing cross-border data transfers

Not having a holistic understanding of all cross-border data transfer activities taking place within their existing systems

Struggling to identify all cross-border data transfer scenarios as a result of a fragmented management approach where different departments or business units conduct their own data transfers

Existing privacy notices, consents and data processing agreements not fully addressing regulatory requirements related to cross-border data transfer

Systems and processes may need to be localised to comply with the relevant regulatory requirements on cross-border data transfers, depending on the actual set up and arrangement of the organisation.

How We Can Help

KPMG offers a range of services to help organisations address concerns and facilitate compliance with the relevant regulatory requirements, including:

Establishment of inventories

Establish inventories for the processing of regulated data and identify situations that require additional measures for cross-border data transfer compliance

Process analysis

Analyse and assess existing business processes against cross-border data transfer principles, taking into consideration the applicable regulations as well as the organisation's development needs

Assessment

Conduct assessment for the impacted business processes and data against cross-border data transfer restrictions to identify potential gaps and plan for remediation actions required

Compliance support

Assist organisation in preparing for compliance activities required by local authorities

Future TOM design

Provide assistance in designing target operating models (TOM) by establishing, updating, localising management frameworks and supporting procedures.

Leverage technical measures to support the future state of TOM, such as segregated systems and data storage with gateway to ensure that only minimum data is being transferred.

Contact us

Jia Ning Song
Partner, Head of Advisory, Hong Kong
KPMG China
T: +852 2978 8101
E: jianing.n.song@kpmg.com

James Zheng
Partner, Head of Management Consulting
KPMG China
T: +86 21 2212 3630
E: james.zheng@kpmg.com

Tom Jenkins
Partner, Head of Banking and Asset Management Risk Advisory and Head of Financial Risk Management
KPMG China
T: +852 2143 8570
E: tom.jenkins@kpmg.com

Henry Shek
Partner, Cybersecurity
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Lanis Lam
Partner, Cybersecurity
KPMG China
T: +852 2143 8803
E: lanis.lam@kpmg.com

Brian Cheung
Partner, Cybersecurity
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

Richard Zhang
Partner, Cybersecurity
KPMG China
T: +86 21 2212 3637
E: richard.zhang@kpmg.com

Quin Huang
Partner, Cybersecurity
KPMG China
T: +86 21 2212 2355
E: quin.huang@kpmg.com

Danny Hao
Partner, Cybersecurity
KPMG China
T: +86 10 8508 5498
E: danny.hao@kpmg.com

Kevin Zhou
Director, Cybersecurity
KPMG China
T: +86 21 2212 3149
E: kevin.wt.zhou@kpmg.com

Corrie Liu
Senior Consultant, Cybersecurity
KPMG China
T: +852 2143 8721
E: corrie.liu@kpmg.com

Shirley Fu
Principal, Legal
SF Lawyers
T: +852 2685 7828
E: shirley.fu@sflawyershk.com

Bessie Chow
Senior Associate, Legal
SF Lawyers
T: +852 2685 7974
E: bessie.chow@sflawyershk.com

kpmg.com/cn/socialmedia

http://www.sflawyershk.com