符涉莉律師事務所
SF Lawyers
In association with KPMG Law

China's new draft Data Privacy law: impacts for financial services sector

Introducing the Personal Information Protection Law

Why get tougher now?

A brief look at China's history with data privacy and security laws will find that the rules surrounding the topic span a number of laws and regulations, such as the General Principles of Civil Law, Tort Liability Law and more recently, the Cybersecurity Law. There are also a number of national standards and sector specific pieces which also govern this topic. Navigating this myriad of complex regulatory rules is becoming increasingly challenging.

The new draft Personal Information Protection Law (PIPL), released on 21 October 2020 is meant to clarify certain aspects of compliance in China in terms of data privacy. In many ways, the situation is likely to be analogous to the impacts felt across Europe with the introduction of the General Data Protection Regulations more than 2 years ago.

Financial Institutions directly impacts

The Growing Responsibilities of Financial Institutions

Even before the PIPL, participants in the financial services sector were classified as Critical Information Infrastructure Operator (CIIOs). CIIOs are entities which are deemed those that, if there is a data leakage or destruction, it would seriously damage China's national security, economic or public interest. This is not surprising given that 80% of all adults in China are bank account holders, and 57% of them use internet banking to make purchases or pay bills*.

Under the PIPL, additional obligations have explicitly been imposed on CIIOs. Primarily, there are new obligations when conducting cross-border data transfers, including separate notice and consent obligations and prior risk assessment and record keeping requirements.

Currently, the People's Bank of China (PBOC) and the Cyberspace Administration of China (CAC) are the two main regulatory bodies for cross-border data transfers in the financial services sector. However, the rules issued by PBOC and CAC are different in certain aspects, such as the scope of data recipients and security assessment requirements. It remains to be seen as to whether this dual-track approach can be unified under the comprehensive PIPL.

* Souce: The World Bank, The Global Findex Database 2017

Serious consequences of non-compliance

What can possibly go wrong if we stay the way we are?

Well, quite a bit actually.

Under the draft PIPL, a financial institution which illegally processes personal data or fails to take necessary data protection measures may be subject to a fine up to RMB 1 million. In serious cases, the fine may be increased up to RMB 50 million or 5% of the financial institution's annual turnover for the previous financial year. In addition, the business license of the financial institution may be revoked and its business operations may have to be suspended as a result. Reputational damage may also be significant.

Existing data collection practices may need enhancement

While the concept of data privacy laws has been around for quite some time, its significance has generally trailed technological advancements. The past decade has seen an era of digital advancement, and particularly for banks, things have changed rapidly. For example, the developments in internet banking, touchless payment systems and online/automated marketing. To provide these services, a huge volume of personal data has been collected.

This rapid change without explicit rules and regulations has meant that different financial institutions have devised their own systems for handling large volumes of personal data. In some cases, different teams within the same financial service institution would deal with personal data differently. The issue is further complicated when financial institutions outsource certain functions and provide personal data to third-parties.

Under the draft PIPL, financial institutions are required to conduct a risk assessment prior to providing personal data to third-parties and retain the records for at least 3 years. Separate prior consent must also be obtained from the relevant individuals. The draft PIPL further introduces certain statutory rights of individuals that are new to Chinese law, such as the right to withdraw consent for any consent-based data processing activities.

Given these requirements, financial institutions have to act quickly, firstly to identify the personal data it (including its affiliates and contracted third-parties) holds, and secondly to organise it in such a way that it becomes manageable and not susceptible to loss.

Financial institutions will also need to reassess their strategies in relation to data collection and methods of retention. They may also need to consider the impacts of the draft PIPL on information already held at the time the new law commences.

What if we are a foreign financial institution?

Modern day technology has helped financial institutions tap into the Chinese market, even when their physical presence in China may be rather limited. Take for example the provision of banking products, life and other insurance products, or asset management, trust or custody services to Chinese consumers. In the course of their services, many of these foreign financial institutions collect the same types of personal data as any local financial institution to market and sell their products to Chinese citizens.

Under the draft PIPL, even if a foreign financial institution has no physical presence in China, as long as it processes personal data of Chinese individuals to provide products or services to individuals in China, or it analyses or assesses the behaviour of individuals in China, or for other specified purposes under Chinese law, it will be captured by the PIPL. This can potentially impact not only on the branch or legal entity carrying on business in China, but its parent and other group companies too.

From another perspective, financial institutions are often key sources of information on individuals. It is therefore very common for foreign regulators operating in areas like banking, insurance, and taxation regulation to request information relating to certain individuals. For foreign financial institutions, especially if a request is received from its home country, the urge to immediately comply with the request may be significant. However, under the new PIPL, the provision of personal data of Chinese individuals relating to requests of foreign governments may be subject to approval from Chinese authorities, i.e., the CAC and its local counterparts.

The need for change

What is becoming obvious is that governments around the world are taking data privacy extremely seriously and it is for good reason. Personal data has much more use cases than one or two decades ago. The advancement of technology has turned personal data from mere data to a key to a person's private life, wealth and livelihood, and unlike other "keys", it is not one which you can simply lose and replace.

While new laws and regulations such as the PIPL add yet another layer to an already complex regulatory compliance environment, here at SF Lawyers we try to adopt a practical approach to assist you in adjusting to these new laws.

Our team at SF Lawyers are experts in data privacy and can assist you in the following:

- Strategic regulatory compliance advice
- Development of security and privacy policies, best practices and procedures
- Data protection program development, including supporting consumer engagement activities such as marketing and advertising
- Data protection, privacy and cybersecurity audits, compliance risk assessment and remediation
- Investigation, containment and remediation of sophisticated data breaches and cybersecurity incidents

SF Lawyers' main point of difference lies in our ability to deliver a 'one stop shop' solution to clients, through our lawyers working seamlessly with KPMG professionals. That is, in leveraging KPMG's significant investments in the areas of cybersecurity and data privacy.

Contact us

Feel Free contact our experts in data privacy for a discussion.

.

Leo Tian
Partner
SF Lawyers
T: +852 2847 5185
E: leo.tian@kpmglegal.com.cn

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

www.kpmglegal.com.cn/hk/en/