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

China's new draft Data Privacy law: impact on life sciences sector

Why get tougher now?

A brief look at China's history with data privacy and security laws in the life sciences sector will highlight that the rules surrounding the topic span a number of laws ,regulations and national standards, such as provisional measures for the administration of human genetic resources, cybersecurity law, tort law, and personal information security. To navigate through, and ensure compliance with, these laws is complex.

The new draft Personal Information Protection Law (PIPL), released on 21 October 2020 is intended to bring together this myriad of different requirements, and to clarify certain aspects in terms of data privacy requirements. In essence, the PIPL is China's equivalent to the General Data Protection Regulations we witnessed in Europe more than 2 years ago.

Life science businesses directly impacts

Even before the PIPL, organizations in the healthcare sector and pharmaceutical research and manufacturing organizations were classified as Critical Information Infrastructure Operators (CIIOs) as its damage, dysfunction or data leakage could severely jeopardize national security, people's livelihoods and the public interest. 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.

Clarifying the scope and processing rules for sensitive data

Personal health and physiological information, personal biological identification information, and human genetic resources in the life sciences sector are classified as sensitive data. The draft PIPL requires data processors who process sensitive personal data to obtain express consent with no exceptions, and provide the specific reasons for processing such data and its implications. More onerously, data processors are required to conduct a prior risk assessment and maintain the records for at least 3 years. Network operators must encrypt the data when transmitting or storing sensitive data.

The draft PIPL stipulates much higher requirements for the life science businesses given the sensitive data they typically possess. The draft PIPL also stipulates that the installation of image collection and personal identification equipment in public places must be necessary to maintain public safety. The term "public safety" has a broad meaning, and it is open to question whether the collection of such information in public places in hospitals meets these requirements.

Life sciences businesses will need to consider their strategies in relation to data collection and methods of processing to ensure compliance with the PIPL.

What if we are a foreign life science business?

The general rule contained in the draft PIPL is that businesses, including foreign businesses, may be impacted, where they obtain the personal data of Chinese individuals to provide products or services to individuals in China, or to analyze or assess the behaviour of individuals in China or for other specified purposes under Chinese law.

Under the draft PIPL, CIIOs and certain processors of personal data must store personal data collected or generated in China within China. The export of personal data is only possible if the export is commercially necessary and has passed a security review.

In practice, R&D centers of a life science business are not always located in the immediate vicinity of where the data is collected. As such, the cross-border transfer of scientific data will often be necessary for R&D purposes. However, not all scientific data is allowed to be transferred cross-border if the scientific data involves personal data .

Under the draft PIPL, certain types of data such as "human genetic resources" requires prior approval by the competent authority for any cross-border transfer. Affected businesses will need to identify and categorize the healthcare data circulated within the entity and fulfill the respective obligations set forth by relevant provisions on cross-border transfer. Additionally, in cases where personal data is concerned, explicit consent must be obtained from individuals. Any big data transfer in the healthcare sector will invariably be required to undergo security assessments before a cross-border transfer is permitted.

What can possibly go wrong?

Under the draft PIPL, a company in the life science sector 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 company may be revoked and its business operations may have to be suspended as a result. Reputational damage may also be significant if there is a breach.

importantly, if the company has an appropriate compliance program to protect personal information under the draft PIPL, the liability may be mitigated or exempted. Therefore, it's essential for the companies in the life sciences sector to put in place appropriate compliance programs under Chinese laws.

The need for change

China is speeding up its legislative processes covering personal data protection, leveraging similar mechanisms implemented elsewhere around the world (including the GDPR in Europe). Here at SF Lawyers, we 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
- Management of employee information and patient medical records
- Development of security and privacy policies, best practices and procedures
- Cybersecurity and privacy contract development and negotiation
- Data protection, privacy and cybersecurity audits, compliance risk assessment and remediation
- Proactive incident response planning

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 to 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/