Ken Dai & Jet Deng

'A 15-Step Guide to Data Protection, Privacy and Cybersecurity in China'

Ever since the PRC Cybersecurity Law (CSL) came into effect on 1 June 2017, China has accelerated its data protection and cybersecurity legislation. Enforcement has gradually been normalised. Meanwhile, the landmark Civil Code – effective as of next year – further strengthens privacy protections from a civil rights perspective. Overall, China is becoming one of the important jurisdictions for data protection and privacy worldwide.

This article gives an overview of data protection, privacy and cybersecurity issues that are common and of concern to enterprises that do business in China. We hope to assist enterprises – especially multinationals – to navigate the increasingly complicated regulatory regime in this field.

1. Understand the Increasingly Comprehensive Legal Regime

China has no single, united data protection law. Rather, its data protection framework consists of a patchwork of fragmented rules found across various laws, measures and sector-specific regulations, with certain overlaps. The CSL is the first national law to address privacy protection and data security. However, quite a few uncertainties around how the law will be applied still remain. Moreover, administrative regulations, ministerial rules and national standards have been introduced by authorities to assist the law's implementation. More and more national standards have been introduced, including the Personal Protection Information Security Specification. Such standards are recommended best practice and not legally binding. Nevertheless, law enforcement authorities have leant heavily on such standards to enforce the CSL. Moreover, as the Personal Information Protection Law and the Data Security Law are being formulated, China's data protection legal regime is expected to become increasingly thorough.

2. Comprehensive Regulatory Authorities

Public enforcement in China presents a polycentric landscape since there is no single data protection or cybersecurity agency. Specifically, the four major authorities involved are the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulations, as well as their local counterparts. In addition, sectoral authorities like the National Health Commission take charge of supervising and administering data protection within their respective fields.

3. App Operation and Privacy Policy

In China, it is necessary to demonstrate a privacy policy in an application if it collects personal information. Since early 2019, CAC and the three other major authorities have engaged in special action ("APP Crackdown") on illegal personal data collection and use by apps. They established a special working group and issued several new guidelines. Currently, enforcement activities against personal information infringement by apps have gradually become normalised and are expected to remain active for the foreseeable future. Thus, multinational companies are advised to ensure their apps are compliant with the relevant laws and guidelines.

4. Multi-Level Protection 2.0

The Multi-Level Protection Scheme requires networks to carry different degrees of protection according to their significance and the severity of the harm caused where they are damaged. Since 2017 the CSL has mandated that China implement multi-level cybersecurity protections. This has meant the prelude to "Multi-Level Protection 2.0". Under this scheme, three important national standards came into force in 2019. It is mandatory for network operators to submit to regulators for Multi-Level Protection filing. The relevant enforcement activities against failure to file are on the increase and should be paid attention to.

5. CIIO Determination

According to the CSL, critical information infrastructure operators (CIIOs) shall be subject to higher cybersecurity requirements and stricter restrictions on cross-border data transfer, compared with general network operators. Meanwhile, the CSL provides that critical information infrastructure (CII) shall refer to networks or systems that involve public communication and information services, energy, transportation, water resources, finance, public services and e-government affairs. They should protect against "damage, dysfunction or data leakage which may severely endanger national security, national economy and the people's livelihood, or public interests". However, as these definitions are quite general, specific rules on CII/CIIO determination are likely to be clarified further in the future.

6. Data Localization and Data Cross-border Transfer

Pursuant to Article 37 of the CSL, CIIOs bear an obligation of data localisation, under important data and personal information collected and generated during the CIIOs' operation in China shall be stored in China. Where such data has to be transferred abroad for business purpose, security assessment shall be conducted pursuant to the relevant rules. Following the CSL, three draft supplementing regulations and guidelines were issued, which expanded the applicable scope of security assessment from CIIOs to general network operators. But none have yet been finalised. Besides, sectoral restrictions on data exports shall be noted when dealing with special categories of data, such as "human genetic resources".

7. Data Protection Impact and Business Innovation

Similar to the data protection impact assessment and privacy by design under the EU General Data Protection Regulation, China's national standard Personal Information Security Specification (PISS) introduces mechanisms for "personal information security impact assessment" and a "personal information security project". Such mechanisms require enterprises to assess the possible impacts on personal information in advance. They should integrate privacy into their business innovations so that potential privacy risks can be identified and solved at an early stage. Notably, such national standards have no legal force, but reference to it is highly significant in practice.

8. Data Protection Officers and Data Governance

Although the concept of a Data Protection Officer has no identical counterpart in the Chinese law, relevant laws and regulations demand "data security positions". For example, the CSL requires the designation of a "person in charge of network security". Similarly, the Provisions on Children's Online Personal Information Protection requires a "person in charge of children's personal information protection" to be designated. Additionally, the latest PISS, effective as of 1 October 2020, clarifies requirements and criteria for designating a department and personnel responsible for personal information protection as well as their responsibilities.

9. IT Global Procurement and Local Adaption

In terms of global IT procurement, special attention should be paid to the network products and

services' server locations as they may involve cross-border data transfers. Furthermore, if a company is a CIIO, greater requirements must be followed. The CSL requires that any purchase of network products and services by CIIOs that may impact national security shall be subject to a security review procedure. The Measures on Cybersecurity Review – effective from 1 June 2020 – elaborates the applicable scope, procedure and factors of such cybersecurity reviews.

10. Data Breach and Cybersecurity Incidents Response

The CSL requires network operators to develop an emergency response plan for cybersecurity events. They must respond promptly to security risks such as system bugs, computer viruses, network attacks and intrusions. In the event of a threatened cybersecurity breach, the operator concerned shall immediately initiate the emergency plan and take corresponding remedial actions. They shall also report the event to the relevant competent authority. On this basis, CIIOs shall also organise regular cybersecurity emergency response drills. On top of this, a draft CII regulation provides that, the competent authorities of industries and sectors shall establish their warning and information reporting systems and emergency response plans for CIIs. Therefore CIIOs will be required to pay attention to the relevant requirements made by the sectoral authorities as well.

11. Sectoral Regulation

The CSL and its supporting regulations are generally applicable to all walks of life. However, different industries may have different degrees of emphasis according to their respective characteristics, especially those handling sensitive information. For example, in health care, pharmaceutical data, medical records and other health care-related data shall be protected according to the relevant department rules. Similarly, finance, education, transportation and other industries have their own sectoral regulations on data protection, which shall be complied to by enterprises in the industries.

12. Criminal Enforcement of Data Protection

Infringing citizens' personal information may incur criminal liabilities. The violating company may be fined and persons directly responsible may be sentenced to up to seven years in prison or given fines and life bans on holding certain critical positions. As such, effective compliance policies should be introduced and implemented to distinguish corporate behaviors from employees' individual behaviors. Besides, Chinese criminal law stipulates "refusing to perform the obligations of information network security management" as a crime under which the failure to perform relevant obligations, such as multi level protection filing, may lead to fines against the company. Persons directly responsible or in charge may be sentenced to fixed-term imprisonment of not more than three years, detention or public surveillance and fines.

13. Corporate Liabilities and Exposure to Senior Management

Under the CSL, a failure to comply with the relevant data protection and cybersecurity requirements may result in harsh administrative penalties for both companies and directly responsible individuals. Specifically, the violating company may be warned and ordered to make rectifications; have illegal gains confiscated; be subject to suspension of business, website shutdown and/or business license revocations; and be fined up to RMB 1 million (roughly USD 146,200). Furthermore, such penalties will be recorded in the company's credit file and made public. Meanwhile, directly responsible persons may be warned, detained, fined up to RMB 100,000 (USD 14,620) and prohibited from holding key positions in cybersecurity for up to five years.

14. Big Data and Competition

Data has been recognized as a factor of production at the national level and the idea of data assets is widely accepted. Companies now compete for data assets and the battles over data present legal issues

concerning ownership and competition law. Although the relevant laws lag behind, in practice some looming rules have been drawn up to help define the boundary of what can and cannot be done with data assets. These include restrictions on using web crawler technology found in civil litigations. It is expected that the traditional rules under the existing competition laws and regulations will be adjusted and updated to apply to the digital realm in the future.

15. Private Enforcement and Collective Redress

Private litigation is always a powerful weapon for big corporations, not least where data is concerned. In recent years, due to an increasing awareness of the importance of personal information protection, individuals are coming forward to bring cases to the courts. This makes data compliance more pressing than ever before. Notably, public interest litigation (PIL) under the PRC Consumers Interests Protection Law has emerged to seek collective redress. Although PILs over data protection are still in their infancy in terms of its quantity, it is predicted that their numbers will continue to grow alongside the development of China's data protection regime.

Conclusion and Look Forward

The Covid-19 pandemic has accelerated the digital transformation of most industries. Enterprises may thus face intensive compliance issues regarding data protection. Therefore, we suggest undergoing a comprehensive examination to identify and avoid any potential risks at an early stage. With the future promulgation of the Personal Information Protection Law and the Data Security Law, businesses may face even greater challenges regarding data compliance. It is the time to take China's data privacy and cybersecurity laws more seriously than ever.