China's cybersecurity and data legal developments and implications for businesses

October 2022

Executive summary

China is proposing amendments to its Cybersecurity Law to increase the penalties for individuals and companies. The Cybersecurity Law has been strictly enforced since it came into effect on 1 June 2017. The other key laws in this space, the Data Security Law and the Personal Information Protection Law, have also been strictly enforced by Chinese regulators since they came into effect at the end of 2021. Recent hefty penalties imposed on various companies and their management have demonstrated the robust enforcement approach taken by the regulators. Businesses should be aware of their compliance obligations in order to avoid enforcement actions.

Obligations for companies

The Cybersecurity Law imposes data security requirements on "network operators". However, the term "network operators" is very broadly defined to include owners, managers, and "service providers" of networks, i.e. "systems comprised of computers and other information terminals and related equipment" that gather, store, transmit, exchange, and process information. This definition not only covers telecommunication, wireless communication, and internet service providers but could ostensibly cover every organisation or business that owns or operates an IT network in China.

Under the Cybersecurity Law, "network operators" are required to comply, *inter alia*, with the following cybersecurity obligations:

- Internal security management systems and operating rules must be implemented, including the requirement to adopt technical measures to prevent viruses and other intrusions; store network logs for at least six months; adopt measures such as data classification systems; and implement security measures such as backup systems and encryption. These data security procedures must be implemented according to China's cybersecurity standard called Multi-Level Protection Scheme ("**MLPS**");
- Emergency response plans must be developed for network security incidents, and in the event of an incident, promptly implement remediation measures and report such incidents to the relevant authorities; and
- Technical support and assistance must be provided to public security agencies to preserve national security and investigate crimes.

Obligations for critical information infrastructure operators

The Cybersecurity Law imposes additional data security requirements on "critical information infrastructure operators" ("**CII operators**"). Critical Information Infrastructure ("**CII**") is defined as important network facilities and information systems in the industries of public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defence, science and technology as well as those that may seriously endanger national security, national economy and the livelihood of the general public, and public interests in case of damage, loss of function or data leakage. Industry regulators are responsible for giving guidance and issuing detailed catalogues of CIIs within their own industries.

CII operators must:

- Undertake additional security measures including conducting security background checks on responsible personnel in critical positions, carry out network security education and technical training, and implement disaster recovery backups;
- Undergo a national security review by the Chinese authorities when purchasing network products or services that might impact national security; and
- Conduct inspections of their network security on at least an annual basis.

Data localisation

Outbound transfer of data from China is a key concern for multinational companies in all industries. Under the China Cybersecurity Law, Data Security Law and Personal Information Protection Law, the transfer of certain data outside of China requires prior Chinese government approval (which is called a "security assessment" under Chinese law). The consent of the individual is not sufficient. A security assessment is required under the following circumstances:

(1) the transfer of personal data or other data outside of China by a CII operator;

(2) the transfer of "important data" outside of China by a data controller (including one that is not a CII operator) ("important data" is broadly defined as data that may endanger national security, economic operation, social stability, public health, and safety once they are tampered with, destroyed, leaked, or illegally obtained or used illegally);

(3) the transfer of personal or other data to a foreign law enforcement or judicial body by any person;

(4) the transfer of personal data outside of China by a data controller (which is called "data processor" in Chinese law) who processes personal information of at least one million people; and

(5) the transfer of personal data outside of China by a data controller who has since 1 January of the preceding year:

  (i) cumulatively provided personal information of 100,000 individuals outside of China, or

  (ii) cumulatively provided sensitive personal information of 10,000 individuals outside of China.

The Chinese regulator (Cyberspace Administration of China) may in future prescribe additional situations which would require a security assessment.

If a company does not fall within any of the foregoing situations, it may utilise one of the following permissible mechanisms to transfer personal information outside of China:

- Certification by a certification organisation to be appointed by the Chinese regulator; or
- Entering into a standard contract ("**Chinese SCCs**") to be prescribed by the Chinese government with the overseas recipient.

Other permissible mechanisms may be prescribed by the Chinese government in the future.

Detailed rules on the three mechanisms (i.e. security assessment, certification or entering into the Chinese SCCs) for outbound data transfer have just been issued by the Chinese government which would inform on the data compliance work of companies.

In addition, prior to outbound transfer of personal data from China, companies need to: ensure that the outbound transfer is necessary; conduct an impact assessment (records of which should be retained for at least three years); provide proper notice to the individual (including name and contact information of the overseas recipient, purpose and method of processing, type of personal information and process for how the individual may exercise his/her rights); and obtain proper, not bundled, consent (which is called "Separate Consent" under Chinese law) from the individual.

Handling of personal information

The Cybersecurity Law, the Data Security Law and the Personal Information Protection Law impose a host of data protection requirements on companies, including abiding by the principles of legality, propriety, and necessity in data handling and also making publicly available privacy notices that explicitly state the purpose, means, and scope for collecting and using information. Companies have been penalised for not complying with these requirements. Individuals, furthermore, are afforded the right to access, modify, and delete their personal information.

Companies are prohibited from transferring personal information without the consent of the individual unless such information has been processed so that the specific individual is unidentifiable and cannot be recovered. Businesses have voiced concerns that

such a legal requirement can be an insurmountable obstacle to the transferring of personal information as it is, in practice, difficult to obtain consent from all relevant individuals.

Identity verification of internet users and instant messaging service users

The Cybersecurity Law has imposed on service providers the responsibility of verifying users' real identification prior to providing services.

MLPS

Under MLPS, companies must conduct assessments of their information systems and the risks associated with them. MLPS have five network security levels based on the damage that would be caused to national security, social order, or public interest in the event of network disruptions or cybersecurity incidents. Each information system is assigned a “level” based on the importance of the system and data and the potential impact of the exposure. Information systems categorised as level 3 or higher must be independently evaluated by a professional, licensed Chinese information security assessment organisation, and information systems categorised as level 2 or higher must be recorded with the Chinese Public Security Bureau. More importantly, companies must perform their security protection obligations in accordance with the requirements of MLPS. China has updated its MLPS cybersecurity standards and refers to the updated MLPS system as MLPS 2.0.

Investigations and penalties

Companies can expect the increased regulatory oversight to continue and intensify as the laws provide regulatory authorities with more explicit and wider monitoring, investigative, and enforcement powers. Companies are required to cooperate with the authorities. Failure to cooperate with the authorities would attract penalties against the companies as well as the responsible individuals.

Non-compliance triggers a wide range of potential penalties for companies, including warnings, suspension of operations, imprisonment, and fines up to RMB 1 million (~USD 150,000). The proposed amendments to the Cybersecurity Law increase the fines against companies to as high as RMB 50 million or 5% of turnover of the previous year, and fines against individuals to RMB 1million. In addition, individuals may also be blacklisted from holding important positions for a certain period of time. The Cybersecurity Law also imposes penalties (such as the freezing of assets) against foreign organisations or individuals who attack or otherwise endanger China's CII.

Potential implications

The consultation on the proposed amendments to the Cybersecurity Law ended on 29 September 2022. It is expected that the amendments will be adopted by the end of the year. Multinational companies across all industries and sectors need to closely review their data security systems and privacy policies for possibly significant changes as the Chinese regulators are vigorously enforcing the laws and the penalties are hefty. Special care must be taken to meet the data localisation requirements, including mapping data for outbound transfer from China, assessing whether Chinese government approval is needed, conducting cross-border data transfer assessments and utilising the permissible mechanisms for outbound data transfer.

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

PwC China

Chun Yin Cheung
Partner
PwC China
+86 (21) 2323 3927
chun.yin.cheung@cn.pwc.com

Tiang & Partners

Chiang Ling Li
Partner
Tiang & Partners
+852 2833 4938
chiang.ling.li@tiangandpartners.com

www.pwccn.com

www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所