Source: *The Business Times,* p17
Date: 21 February 2023

Navigating China's new cross-border data transfer rules

The tightening of data flow policies in China spells implications beyond those for multinationals operating in the country.

BY XIE TAOJUN, LIU JINGTING, ULRIKE SENGSTSCHMID, GE YIXUAN

AS GLOBAL digital economy integration deepens, China is tightening cross-border data transfers through new regulations.

China recognises the importance of data in driving domestic economic growth. In December 2022, the Central Committee of the Chinese Communist Party and the State Council reaffirmed data to be a new type of production factor, and encouraged data sharing to unleash its full economic value. But cross-border data transfers are subject to strict controls.

The latest addition to China's regulatory framework are the updated Security Certification Specifications released on Dec 16, 2022, setting the standards for agencies certifying companies' cross-border data transfers. Earlier on Sep 1, 2022, the Measures for Data Export Security Assessment took effect, regulating when companies must undergo a security assessment with China's cyberspace authority. Both regulations pertain to Article 38 of China's Personal Information Protection Law (PIPL) passed in 2021, which stipulates the conditions for exporting data abroad.

The Measures for Data Security Management in the Field of Industry and Information Technology – which outline security requirements for industrial, telecom, and radio communication data – also just came into force on Jan 1, 2023, complementing the Data Security Law (DSL) passed in 2021.

Together, the Cybersecurity Law (CSL) passed in 2017, the DSL, and the PIPL form the three pillars of China's data protection legislation, under which transferring data out of China has become substantially more difficult.

Yahoo cites the "increasingly challenging business and legal environment" as the key reason for shutting its online services and completely withdrawing from the Chinese market in November 2021. PHOTO: BLOOMBERG

Stringent mechanisms for external data transfers

Besides mandating data handling requirements to ensure data protection and consent, the PIPL stipulates three ways under which companies can transfer data out of China.

First, a firm can pass the cyberspace authority's security assessment. This is mandatory for critical information infrastructure operators, firms processing "important" data, or firms handling data volumes above pre-determined thresholds.

"Important" data is defined rather vaguely as pertaining to national security and major public interests, leaving authorities interpretative leeway but also increasing uncertainty for firms.

Second, a China-based affiliate of a multinational company can obtain a personal information protection certification. This affiliate is then legally responsible for the multinational's cross-border data processing.

Third, the entities sending and receiving data can sign a standardised contract and conduct a Personal Information Protection Impact Assessment. While this approach is arguably the easiest, only companies excluded from security assessments are eligible.

Comparing the PIPL with the GDPR

Somewhat surprisingly perhaps, China's PIPL seems to resemble closely the European Union's trailblazing General Data Protection Regulation (GDPR). But using similar personal information definitions and consent requirements lowers compliance costs for international firms and increases interoperability.

However, despite these surface-level similarities, the EU regulates data privacy while maintaining relatively free cross-border data transfers, whereas China imposes restrictions on international data flows in the interests of national security.

Rather than assessing data transfers on a case-by-case basis like China, the GDPR allows for unrestricted data transfer to 14 non-EU countries with comparable data protection levels. Additionally, multinationals can transmit data to third countries under appropriate standard contracts, binding corporate rules, or codes of conduct. Data localisation is generally not required by the GDPR.

China's rationale

There is no doubt that China's data flow policies stem from national security concerns. Already in 2018, President Xi Jinping emphasised that "there is no national security without cybersecurity". Since then, the recognition of the value of data and risks of cyberattacks have only increased. Thus, China's new data protection framework aims to carefully balance China's economic growth imperatives with its national security interests. China may not be the only country adopting such a stance, but its regulations are highly restrictive.

In contrast to its restrictive stance internationally, the Chinese government is driving better utilisation of the country's data resources and encouraging smooth data flows domestically. Last year, the Shenzhen data exchange was established to facilitate data trading – similar to commodity trading – boosting domestic firms' productivity.

Implications for cross-border service providers

Data is a key factor of production in the digital economy. Provisions of services such as social networking platforms hinge on smooth data transfers. Besides, data-driven business insights enable firms to make better product offerings and improve marketing effectiveness.

With the controls on data export in the country, foreign firms will face difficulties in sharing data generated in their business activities in China with their headquarters and R&D centres located overseas, impeding innovation and affecting their product offerings to Chinese consumers.

Hotels, for example, use customer information stored in their membership databases to provide customised services at any of their branches, which require free data flows. Yet the sheer volume of data processed by large hotels will trigger data localisation requirements.

Medical devices that enable remote monitoring of patients will also need to transmit health metrics to healthcare professionals for assessment. Health data, which may be categorised as "sensitive" data, are subject to stricter regulations.

In the financial sector, wealth management organisations abroad conducting due diligence checks will necessitate the cross-border processing of "sensitive" customer personal information, including financial status, family background, and even health conditions, which requires security assessment once the processing volume reaches a certain threshold.

Compliance with China's data transfer regulations will raise the operating costs of multinationals as new data handling processes are required. This impairs their price competitiveness vis-a-vis domestic firms.

The costly adjustments have deterred some companies. Yahoo, for example, cites the "increasingly challenging business and legal environment" as the key reason for shutting its online services, and completely withdrawing from the Chinese market in November 2021.

Besides foreign multinationals, domestic firms will also face higher costs when tapping into globalised business models and expanding overseas. The unintended longer-term consequence could be impediments to domestic firms' global competitiveness.

Adjusting to the new regulatory regime

With the availability of advanced data facilities domestically – for instance, 5G networks and data exchanges – China has led the development of the digital economy in the world. Its huge consumer market presents many business opportunities for tech companies, some of which have deemed compliance with the regulations worthwhile.

While China's cross-border data transfer regulations are new and still unfolding, some multinationals have adjusted by duplicating data centres, staffing, and key operative processes within the country.

Apple, for example, moved its Chinese users' iCloud data to a dedicated data centre in China in 2018, in response to the CSL's data localisation requirements.

Companies may also create separate product offerings for the Chinese market to circumvent compliance issues, hurting consumer interests and corporate competitiveness in China.

The replacement of LinkedIn with InCareer in China is one example: The new job-posting application without social feeds or post-sharing features introduced in December 2021 for the Chinese market bypasses the data export regulations by completely disconnecting it from the global LinkedIn platform.

Uncertain future

Despite appearing restrictive, the PIPL makes exceptions for overseas data transfers based on international treaties and agreements, preserving some leeway as China enters discussions on digital economy collaborations with global partners. However, when such agreements will be signed and how compliance will work in practice remain to be seen.

Balancing economic growth and competitiveness with national security interests in today's globalised digital economy is difficult.

Exactly which path China will tread will become clearer as authorities begin interpreting and implementing the regulations and assessments. As more jurisdictions roll out distinctive sets of standards pertaining to cross-border data flows, there will be an extended period of uncertainty as global parties look for the optimal policy mix.

The writers are researchers from the Asia Competitiveness Institute, at the Lee Kuan Yew School of Public Policy, National University of Singapore.