WILMERHALE

China Publishes Draft Regulations on the Administration of Network Data Security

December 6, 2021

The Cyberspace Administration of China ("CAC") on November 14, 2021 published the draft Regulations on the Administration of Network Data Security ("Draft Regulations") for comment through December 13, 2021.[1] The Draft Regulations set forth in comprehensive detail provisions to regulate data processing activities in order to implement the Cybersecurity Law ("CSL"), the Data Security Law ("DSL"), and the Personal Information Protection Law ("PIPL"), key provisions of which are reflected in the Draft Regulations. The Draft Regulations contain 75 articles in nine chapters that would provide for personal information ("PI") protection, the security of "Important Data," rules on cross-border data transfers, obligations on Internet platform operators, provisions on government administration and legal liability, and definitions of key terms, including what constitutes "Important Data."

The Draft Regulations have extraterritorial effect, inasmuch as they would apply not only to data processing activities inside China,[2] but also to the processing outside of China of data of persons and organizations inside China if (i) for the purpose of providing products or services to China; (ii) for analyzing or assessing the behaviors of persons and organizations inside China;[3] (iii) in connection with the processing of domestic Important Data; or (iv) in other legally required circumstances (Article 2). Processing activity conducted outside of China which harms China's national security, public interest, or the legal interests of citizens or organizations is punishable under the Draft Regulations (Article 72).

Highlights of the Draft Regulations are set out below.

[1] Request for Comments (Nov. 14, 2021), available at http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm.
[2] China here means the People's Republic of China, which absent specific reference to the inclusion of Hong Kong is generally understood to exclude Hong Kong, Macao, and Taiwan.
[3] Note that this goes beyond Art. 3(2) of the PIPL, the purpose of which is to analyze or assess the behaviors of persons inside China, not the behaviors of persons or organizations inside China. The Draft Regulations therefore arguably have an extraterritorial scope beyond that of the PIPL.

Important Data and Core Data

Definition: The Draft Regulations define the term "Important Data," but the definition is quite broad, perhaps intentionally. Important Data is defined as data that may endanger national security or the public interest if tampered with, destroyed, leaked, or illegally obtained or used, and specifically includes (Article 73(3)):

1. unpublished government affairs data, work secrets, intelligence data and law enforcement and judicial data;
2. export control data; data relating to core technology, design plans, and manufacturing processes in connection with export-controlled items; data on scientific and technological achievements in such areas as encryption, biology, electronic information, and artificial intelligence that have a direct impact on national security and economic competitive strength;
3. national economic operating data, important industry business data, and statistical data subject to protection or under restricted distribution;
4. data on secure production and operation of such key industries and sectors as industry, telecommunications, energy, transportation, water, finance, defense technology industry, customs, and taxation, as well as data on key system components and equipment supply chains;
5. national basic data on population, health, natural resources and environment such as genes, geography, minerals, and meteorology that reach the scale or accuracy prescribed by the relevant government departments;
6. data on the construction, operations and security of national infrastructure and critical information infrastructure ("CII");[4] data on the geolocation or security of important sensitive areas such as national defense facilities, military areas, and national defense research and production entities; and
7. other data that may have an impact on the security of China's politics, land, military, economy, culture, society, science and technology, ecology, resources, nuclear facilities, overseas interests, biology, space, polar regions, and deep seas.[5]

The Draft Regulations define "Core Data" as data related to national security, the lifeline of the national economy, important livelihood of people or major public interests. Core Data receives the highest degree of protection.

[4] CII is defined in Art. 31 of the CSL as important network infrastructure and information systems, the destruction, loss of function or data leakage of which could seriously harm the state security, national economy, people's livelihood and public interest.
[5] This list conforms with the sixteen contemporary dimensions of national security, *see National Security Education Day for All | How much do you know about national security knowledge*, XINHUA (Apr. 15, 2021), available at http://www.xinhuanet.com/legal/2021-04/14/c_1127329200.htm.

Multi-Level Protection Scheme ("MLPS"):[6] Consistent with the CSL and the DSL, network systems and data are to be protected based on MLPS. Systems on which Important Data is processed shall, in principle, meet the security protection requirements of MLPS Level 3 or above and CII. Systems for processing Core Data shall be strictly protected in accordance with relevant regulations (these regulations are unspecified, but may include the Law on Protecting State Secrets (rev. 2010)). Important Data and Core Data shall be protected by encryption (Article 9).

Additional filings and emergency response: Data processors[7] of Important Data are required to submit filings for the record to the municipal cybersecurity administration upon identification of its Important Data (Article 29) and conduct annual data security assessments by themselves or through third-party data security service institutions with an assessment report to be filed with the municipal cyberspace administration (Article 32). Data processors are required to report security incidents that involve Important Data or PI of more than 100,000 individuals within eight hours to the municipal cybersecurity administration and applicable regulatory authorities, and file investigation assessment reports with the same authorities within five working days after the incident has been handled. This reporting requirement is in addition to the requirement to notify the individuals or organizations harmed by the incident within three working days (Article 11).

Procurement requirements: Important Data processors shall give priority to the purchase of secure and trusted network products and services (Article 31). Secure and trusted is not defined in the Draft Regulations but is generally understood to mean domestic products. Government agencies and CII operators ("CIIO") would be subject to joint security review by CAC and the applicable departments under the State Council for the procurement of cloud computing services (Article 34).

PI of more than one million individuals: Data processors that process PI of one million or more individuals would be treated as Important Data processors (Article 26), and therefore subject to stricter scrutiny and compliance requirements.

---

[6] MLPS is a set of compulsory requirements for implementation by network operators in China with respect to their network security, the key legal foundation of which may be found in Art. 21 of the CSL. The scheme ranks network systems on a scale of sensitivity and risk, with Level 1 being the least and Level 5 being the most sensitive and risky. Systems classified at Level 2 or higher are required to engage a qualified expert to conduct additional review and verification, and file for certification with the local public security department. Systems classified at Level 3 or higher are required to conduct re-assessment every year, and implement technical maintenance in China. The current MPLS 2.0 is an update of previously existing regulations dating back to 1994 and 2007, and consists of the draft Regulations on MLPS (2018) issued by the Ministry of Public Security (still in draft form and pending finalization) and effective mandatory national standards issued by State Administration for Market Regulation and Standardization Administration of China including (1) the GB/T 22239-2019 Basic Requirements for the Multi-level Protection of Information Security Technology, (2) the GB/T 25070-2019 Information Security Technology Cybersecurity Multi-level Protection Security Design Technical Requirements, (3) the GB/T 28448-2019 Information Security Technology Cybersecurity Multi-level Protection Assessment Requirements, and (4) GB/T 25058-2019 Information Security Technology-Implementation Guide for Cybersecurity Classified Protection.

[7] The concept of data processor under Chinese law is equivalent to that of Data Controller under the General Data Protection Regulation and does not include the agent that accepts the entrustment of a data processor to handle the data.

Overseas listing: Consistent with the draft amendment to the Cybersecurity Review Measures (2020),[8] the Draft Regulations would impose a cybersecurity review requirement on PI processors of one million or more individuals who intend to conduct an IPO in a foreign country (Article 13(2)).[9] This review requirement would not apply to data processors who intend to list in Hong Kong, however, unless the listing has or may have an impact on national security (Article 13(3)). By subjecting IPOs in a foreign country to stricter scrutiny than IPOs in Hong Kong, this aspect of the Draft Regulations would indirectly encourage the latter for data control purposes. Data processors that intend to list overseas (regardless of whether in a foreign country or Hong Kong) would be required to conduct an annual data security assessment (Article 32). This may signify, however, that the central government authorities have other means to address network data security relating to IPOs by Chinese companies in Hong Kong.

Cross-border transfer: Processors of Important Data would become subject to more stringent compliance requirements regarding the export of Important Data, including (i) conducting a CAC-led security assessment (Article 37(1)); and (ii) filing an annual data export security report to the municipal cybersecurity administration by January 31 of the following year (Article 40).

Cross-border data transfer

Conditions: Article 35 of the Draft Regulations would require data processors to satisfy one of four conditions to transfer data overseas for business or other reasons:

1. ***Pass a CAC-led security assessment:*** Consistent with the draft Measures on the Security Assessment of Cross-Border Data Transfer ("Draft Security Assessment Measures"),[10] Article 37 of the Draft Regulations provides that a CAC-led security assessment shall be conducted (i) when data to be exported contains Important Data; (ii) when PI is exported by CIIOs and data processors who process PI of one million or more individuals; and (iii) in several other scenarios (cross-border transfer of PI of 100,000 or more individuals or sensitive PI of 10,000 or more individuals by any data processor, or transfers that would otherwise implicate national security or the public interest, in accordance with the Draft Security Assessment Measures). These CAC-led security assessments can be burdensome and time-consuming. Therefore, regular data processors (non-CIIO and non-massive PI processor) which transfer regular data (non-PI and non-Important Data) overseas may be reluctant to utilize this option, except where mandated to do so by the Draft Security Assessment Measures.

[8] The current Cybersecurity Review Measures (2020) aims only to subject CIIOs whose purchase of network products and services that has or may have an impact on national security to cybersecurity review. The draft amendment to the Measures expands such cybersecurity review requirement to cover IPOs in foreign countries by PI processors of more than one million individuals, but such amendment remains in draft form and has yet to be finalized.
[9] Foreign country here does not include Hong Kong.
[10] For additional analysis of the Draft Security Assessment Measures, please refer to WilmerHale publication dated Nov. 3, 2021, available at: https://www.wilmerhale.com/en/insights/client-alerts/20201103-china-publishes-draft-measures-on-security-assessment-of-cross-border-data-transfer.

2. ***Data recipient obtains a CAC PI certification:*** This condition goes beyond the PIPL by requiring overseas data recipients, in addition to data processors, to pass PI certifications. This is an exceptionally burdensome requirement that would likely discourage overseas data transfers.

3. ***Use of a CAC standard contract stipulating the rights and obligations of both parties:*** This condition is similar to the comparable condition imposed by the PIPL, and may present a reasonable means for cross-border data transfers, even across borders within multinational corporations ("MNCs"). However, the CAC has not yet issued a standard contract.

4. ***Other conditions as may be stipulated by law, administrative regulation, or the CAC:*** Such other conditions may include self-security assessments conducted by regular data processors when transferring regular data overseas, where no CAC-led security assessment is otherwise required, in accordance with the Draft Security Assessment Measures.

Carve-out: Article 35 of the Draft Regulations would exempt two scenarios from compliance with the above-mentioned conditions on cross-border data transfers – specifically, transfers (i) for the purpose of entering into and performing a contract to which the data subject is a party; or (ii) for the purpose of protecting the life, health and property of an individual. The first exemption in particular would likely reduce the burden for MNCs to share customer and employee PI with overseas headquarters based on sales contracts and employment contracts, but it falls short of covering other data, such as operational, management and sales data, that MNCs regularly share across borders within their organizations.

Notably, Article 38 of the PIPL imposes similar conditions on the overseas transfer of PI. But Article 35 of the Draft Regulations expands these conditions to apply to *all* data without qualification as to its volume or nature (regardless of whether PI, Important Data or regular data), with the exception of the two purposes noted above.

Gateways

Great Firewall: Article 41 of the Draft Regulations would provide a legal foundation for the Great Firewall that has been in existence for the past decade. It would apply in reverse to overseas data, *i.e.*, authorize the State to establish cross-border data security gateways to block information from outside China that is prohibited by laws and administrative regulations from being released or transmitted within China.

VPNs and servers: Article 41 also provides that no party may provide programs, tools, and lines to penetrate or bypass the data cross-border security gateways, or provide Internet access, server hosting, technical support, transmission and promotion, payment settlements, and application downloads for penetrating or bypassing cross-border data security gateways. In addition, when users inside China access networks inside China, their traffic may not be routed overseas.

It is unclear whether this provision would prohibit the use of VPNs in China; if it did, it would directly contradict the Notice on Cleaning up and Standardizing the Internet Network Access Service Market (2017) issued by the Ministry of Industry and Information Technology, which allows officially authorized VPNs to be used for business purposes. It is also unclear if Article 41 would impact MNCs whose servers are hosted offshore.

Conclusion

As currently drafted, the Draft Regulations provide an enhanced framework that would impose stringent requirements on data processors, cross-border data transfers, and IPOs in foreign countries. Although they would clarify many aspects of network data security requirements – such as type of data covered, threshold limits, and conditions on transfer of data – they also would impose difficult government reviews and potential reporting requirements.

Given their scope and likely impact on hardware choices and cross-border data transfers, the Draft Regulations are in tension with China's WTO commitments under the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS). The Draft Regulations are also in tension with China's recently stated desire to become a party to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the Digital Economy Partnership Agreement, two Asia-Pacific regional trade agreements with strong disciplines meant to facilitate digital trade, including cross-border transfers of information.

Contributors

Lester Ross
PARTNER

lester.ross@wilmerhale.com
+86 10 5901 6588

Kenneth Zhou
PARTNER

kenneth.zhou@wilmerhale.com
+86 10 5901 6588

Tingting Liu
COUNSEL

tingting.liu@wilmerhale.com
+86 10 5901 6588