

February 9, 2022

## A Snapshot of China’s Cyberspace Administration and Data Protection Framework

By [Liza L.S. Mark](#) and [Tianyun Ji](#)

China’s triad of cyberspace and data laws passed by the country’s highest legislature – China’s National People’s Congress Standing Committee (“**NPC**”) – are now fully effective: the *Personal Information Protection Law* (《个人信息保护法》), effective November 1, 2021; the *Data Security Law* (《数据安全法》), effective September 1, 2021; and the *Cybersecurity Law* (《网络安全法》), effective June 1, 2017 (collectively, “**Data Laws**”). Together, with their respective implementation rules and regulations by agencies, such as the Cyberspace Administration of China (“**CAC**”), as well as general and industry standards, China’s cyberspace administration and data protection framework poses major compliance challenges for multi-national companies (“**MNCs**”) with operations in China.

Unfortunately, the Data Laws mainly set out the general framework for regulation of data in China, with detailed implementation guidelines still to be provided further by implementing regulations and industry standards. Hence, there remains a great deal of ambiguity as to specific requirements and what companies need to do with respect to their internal compliance on data security and personal information protection. Here, we are trying to provide MNCs with a snapshot overview as a reference tool to understand the big picture of China’s existing and ongoing legislation regarding data protection, without getting into too much detail of each such rule.

The chart below provides key preliminary issues for MNCs to consider when attempting to comply with the Data Laws:

	<b>Cybersecurity Law (2017)</b>	<b>Data Security Law (2021)</b>	<b>Personal Information Protection Law (2021)</b>
<b>Who needs to comply?</b>	<p><b>Network Operator:</b> those that construct, operate, maintain and/or use a network in China.</p> <p><b>CIIO<sup>1</sup>:</b> those Network Operators that are involved with critical information infrastructure.</p>	<p><b>Data Processor:</b> those who collect, store, use, process, transmit, provide and publicize data<sup>2</sup>.</p>	<p><b>PI<sup>3</sup> Processor:</b> those who collect, store, use, process, transmit, provide, publicize, delete personal information<sup>4</sup>.</p>

1 Critical Information Infrastructure Operator.

2 “Data” means any recording of information by electronic or other means.

3 Personal Information.

4 “Personal Information” means all types of information relating to identified or identifiable individuals that is recorded by electronic or other means, excluding anonymously processed information.

# HAYNES BOONE

<b>Jurisdictional applications</b>	<b>In rem</b> (i.e., The law applies to the construction, operation, maintenance, and use of networks in China.)	<b>In rem</b> (i.e., The law applies to data processing activities in China, but the law also applies to processing activities outside of China which harm China’s national security, public and private interests).	<b>In rem</b> (i.e., The law applies to PI processing activities in China); and <b>In persona</b> (i.e., The law also applies to processing activities outside of China, if (i) they provide products or services to individuals in China; or (ii) they analyze and evaluate behaviors of individuals in China).
<b>Onshore storage of data</b>	CIIO shall store onshore PI and important data <sup>5</sup> that is collected and generated in China.	Unspecified, but the same requirements in the Cybersecurity Law apply.	Mandatory onshore PI storage for CIIO.
<b>Data export</b>	Need to conduct security assessment first, before transmitting PI and important data that are stored onshore.	For CIIOs exporting important data collected and generated in China, the same standards apply as in CSL. For non-CIIOs exporting important data, they will be further regulated by CAC. In addition, one (CIIO or non-CIIO) needs to obtain prior approval from authorities before providing data stored in China to foreign judicial or law enforcement agencies.	- Transferring PI is allowed if it meets one of the following conditions: (i) after conducting a security assessment (for CIIOs); (ii) obtaining certification for transferring PI from accredited agencies; or (iii) having a contract regarding transferring PI per model contract by CAC. Before transferring PI cross-border, one needs to obtain an individual’s prior consent, by notifying them of: overseas recipient’s name, contact information, processing purpose, method, type of PI, and rights and obligations. - Need to obtain prior approval from authorities before providing PI to foreign judicial or law enforcement agencies.

<sup>5</sup> Currently, what is considered “important data” is still not clear. In 2022, we expect that China will provide clearer guidance on defining “important data” by finalizing and implementing industry standards such as the Identification Guide for Important Data (Exposure Draft) (《信息安全技术重要数据识别指南（征求意见稿）》) and the Practical Guide for Cybersecurity Standards-Data Classifications (《网络安全标准实践指南—数据分类分级指引》) that are discussed further below in this article.

# HAYNES BOONE

<b>Penalties</b>	Various fines range from RMB 5,000 to RMB 1,000,000 to companies and individuals, suspension of business license, shutdown of business, criminal liabilities, etc.	Violation concerning “core data:” fine up to RMB 10 million (approx. US\$1.6 million), suspension of business and potential criminal liabilities. Violation concerning “important data:” fine up to RMB 5 million (approx. US\$780,000).	For companies: fine up to RMB 50 million (approx. US\$7.8 million) or 5% of its annual turnover in the preceding year, disgorgement of illicit gains, etc. For individuals: fine up to RMB 1 million and a ban from serving in a managerial role in the organization.
------------------	--	---	--

In addition to the high-level laws passed by the NPC, a handful of implementing rules and industry standards for more detailed guidance and instructive implementations have either come into effect or are in the pipeline. Below are notable examples:

<b>Name</b>	<b>Promulgating Authority</b>	<b>Status</b>	<b>Description</b>
<i>Security Protection Regulations for Critical Information Infrastructure</i> 《关键信息基础设施安全保护条例》	State Council of the PRC	Effective September 1, 2021	Guidance on who determines which entity is considered a “CIIO,” how such determination is made, and the detailed description of the CIIO’s obligations in safeguarding security.
<i>Several Provisions on Automotive Data Security Management (for Trial Implementation)</i> 《汽车数据安全 若干规定 (试行)》	CAC, NDRC <sup>6</sup> , MIIT <sup>7</sup> , MPS <sup>8</sup> and MOT <sup>9</sup>	Effective October 1, 2021	For the first (and so far, the only) time defines “important data” for a particular industry. It further provides detailed guidance for the auto industry in classifying “PI” and “important data.”

6 National Development and Reform Committee of China.

7 Ministry of Industry and Information Technology of China.

8 Ministry of Public Service of China.

9 Ministry of Transportation of China.

# HAYNES BOONE

<i>Administrative Regulation on the Cyber Data Security (Exposure Draft) 《网络安全数据安全条例 (征求意见稿) 》</i>	CAC	Draft for public comments (published on November 14, 2021)	The draft provides for more detailed regulations regarding various concepts and systems in the Data Laws, such as: a data classification protection system, cybersecurity assessment and foreign public offerings, data export security management, obligations of platform operators, obligations of processor of important data, etc.
<i>Measures for the Security Assessment of Outbound Data (Exposure Draft) 《数据出境安全评估办法 (征求意见稿) 》</i>	CAC	Draft for public comments (published on October 29, 2021)	The draft calls for mandatory self-assessment of risks before transmitting data overseas. A security assessment by local CAC authorities will also be mandatory in the event of exporting data, if meeting one of the criteria below: (i) PI and important data obtained and generated by CIIO; (ii) contains important data; (iii) PI processor of over 1 million PI; (iv) aggregated over 100,000 pieces of PI, or aggregated over 10,000 pieces of sensitive PI; or (v) others as required by CAC.
<i>Cybersecurity Review Measures (Draft Revision for Comment) 《网络安全审查办法 (修订草案征求意见稿) 》</i>	CAC	Draft revision for public comments (published on January 4, 2022)	The draft requires any operator with over 1 million users' PI to file for cybersecurity assessment with the CAC, before going public in a foreign jurisdiction.
<i>Practical Guide for Cybersecurity Standards-Data Classifications 《网络安全标准实践指南—数据分类级指引》</i>	National Information Security Standardization Technical Committee	Published on January 4, 2022	It sets out the principles, framework and rules in classifying different categories of data including PI, "important data," national core data, public data, business data, and derivative data.
<i>Identification Guide for Important Data (Exposure Draft) 《信息安全技术重要数据识别指南 (征求意见稿) 》</i>	National Information Security Standardization Technical Committee	Draft as of October 2021	It sets out the principles and procedures for identifying "important data" and identifies key features of "important data."

Given the declaration in the important policy document, "[Opinions of the Central Committee of the Communist Party of China and the State Council on Improving the Market-based Allocation Mechanism of Production Factors](#) (中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见)," March 30, 2020, where data is listed as one of the five basic factors of production, alongside land, labor, capital and technology, we expect that

# HAYNES BOONE

the regulation of data would only tighten further. Businesses with operations in China should ensure compliance (or at the very least the building block for compliance) with the Data Laws, implementation regulations and industry standards by:

- mapping out the organization's existing data collection and processing operations in China (i.e., data-mapping);
- having dedicated personnel to carry out and implement data security protection and compliance;
- closely monitoring the progress of implementing regulations and measures of the Data Laws and guidelines published by industrial regulatory authorities.

In addition, MNCs that deal with PI or "important data" should be particularly mindful about how to handle cross-border data flows. Some data may now have to be stored locally and will need pre-approval before being transmitted overseas. Businesses should understand and categorize data throughout the organization, identify their obligations under the Data Laws with respect to each type of the data, and develop and implement internal systems to ensure compliance.

For more information, please visit our [China Updates](#) page or see the following resources:

- [China Intensifies Regulations on Cryptocurrency Trading and Mining](#), November 2, 2021
- [China's Amended Administrative Penalty Law Took Effect on July 15](#), October 8, 2021
- [China Issues New Rules Regulating Personal Information Collection by Mobile Apps](#), April 28, 2021
- [A New Gateway to China – Recent Policy Developments in the Hainan Free Trade Port](#), April 6, 2021
- [China Issues Measures for the Security Review of Foreign Investments, February 9, 2021](#)
- [China Patent Law Fourth Amendment—Impact on Foreign Companies](#), January 26, 2021
- [China Regulators Remove Restrictions on Insurance Fund Investment](#), December 14, 2020
- [China Adopts Interim Provisions on the Review of Concentrations of Business Operators for the Anti-Monopoly Law](#), November 30, 2020
- [China Releases Draft Personal Data Protection Law for Comments](#), November 12, 2020
- [China Adopts Export Control Law](#), November 5, 2020
- [China Releases New QFII/RQFII Rules](#), October 27, 2020
- [China Releases Provisions on Strengthening the Supervision of Private Equity Investment Funds \(Draft\)](#), October 15, 2020
- [China Releases Provisions on the Unreliable Entity List](#), October 5, 2020
- [China Releases Revised Measures on Handling Complaints of Foreign-Invested Enterprises](#), September 23, 2020
- [China Releases Administrative Measures for Strategic Investment by Foreign Investors in Listed Companies](#), September 10, 2020
- [China Releases Draft Data Security Law](#), September 8, 2020
- [China Releases Circular on Further Stabilizing Foreign Trade and Foreign Investment](#), August 24, 2020
- [China Releases Draft Measures for the Administration of Imported and Exported Food Safety](#), August 18, 2020
- [U.S. Listed Chinese Companies: Regulatory Scrutiny and Strategic Options](#), July 30, 2020
- [China Passes Controversial Hong Kong National Security Law](#), July 9, 2020
- [China's Relaxed Financial Sector May Aid Foreign Investors](#), June 18, 2020
- [Is There a Law in China Similar to the US Defense Production Act?](#), May 8, 2020
- [Coronavirus Brings Force Majeure Claims to LNG Contracts](#), March 4, 2020

# HAYNES BOONE

- [The Rise of China](#), March 4, 2020
- [Coronavirus Fears Cast Cloud Over Dealmaking](#), February 27, 2020

Additional questions? Please contact Haynes Boone lawyers [Liza L.S. Mark](#) and [Tianyun Ji](#)