GIBSON DUNN

China Constricts Sharing of In-Country Corporate and Personal Data Through New Legislation

Client Alert | June 17, 2021

The People's Republic of China is clamping down on the extraction of litigation- and investigation-related corporate and personal data from China—and this may squeeze litigants and investigation subjects in the future. Under a new data security law enacted late last week and an impending personal information protection law, China is set to constrict sharing broad swaths of personal and corporate data outside its borders. Both statutes would require companies to obtain the approval of a yet-to-be-identified branch of the Chinese government before providing data to non-Chinese judicial or law enforcement entities. As detailed below, these laws could have far-reaching implications for companies and individuals seeking to provide data to foreign courts or enforcement agencies in the context of government investigations or litigation, and appear to expand the data transfer restrictions set forth in other recent Chinese laws.[1]

Data Security Law of the People's Republic of China

On June 10, 2021, the National People's Congress passed the Data Security Law, which will take effect on September 1, 2021. The legislation contains sweeping requirements and severe penalties for violations. It governs not only data processing and management activities within China, but also those outside of China that "damage national security, public interest, or the legitimate interests of [China's] citizens and organizations."[2]

The Data Security Law generally requires entities and individuals operating within China to implement systems designed to protect in-country data. For example, entities that handle "important" data—a term not yet defined by the statute—must designate personnel responsible for data security and conduct assessments to monitor potential risks.[3] Chinese authorities may issue fines up to 500,000 CNY (approximately $78,000) and mandate remedial actions if an entity does not satisfy these requirements.[4] If the entity fails to implement required remedial actions after receiving a warning and/or its failure to implement adequate controls result in a large-scale data breach, the entity may be subject to a fine of up to 2 million CNY (approximately $313,000). Under these circumstances, authorities also may revoke the offending entity's business licenses and issue fines to responsible individuals.[5]

The Data Security Law also states that a "violation of the national core data management system or endangering China's national sovereignty, security, and development interests" is punishable by an additional fine up to 10 million CNY (approximately $1.56 million), suspension of business, revocation of business licenses, and in severe cases, criminal liability.[6] The Data Security Law broadly defines "core data" to include "data related to national security, national economy, the people's welfare, and major public interests."[7]

Most notably, Article 36 of the Data Security Law prohibits "provid[ing] data stored within the People's Republic of China to foreign judicial or law enforcement bodies without the approval of the competent authority of the People's Republic of China."[8] The law does not identify the "competent authority" or outline the approval process. Failure to obtain this

Related People

Patrick F. Stokes

Oliver Welch

Nicole Lee

Ning Ning

Kelly S. Austin

Judith Alison Lee

Adam M. Smith

John D.W. Partridge

F. Joseph Warin

Ryan T. Bergsieker

Stephanie Brooker

John W.F. Chesley

Connell O'Neill

Michael Scanlon

Benno Schwarz

prior approval may subject an entity to a fine of up to 1,000,000 CNY (approximately $156,000), as well as additional fines for responsible individuals.[9] Although the Data Security Law discusses different categories of covered data elsewhere in the legislative text—referring to, for example, the "core data" discussed above[10]—Article 36, as written, appears to apply to the transfer of *any* data, regardless of subject matter and sensitivity, so long as it is stored in China. The final legislative text also includes additional, heavier penalties for severe violations that had not been included in prior drafts, including a fine of up to 5 million CNY (approximately $780,000), suspension of business operations, revocation of business licenses, as well as increased fines for responsible individuals. The statute does not, however, define what violations would be considered "severe."

While the legal community in and outside of China will certainly seek additional guidance from the Chinese government, it is unclear whether the Chinese government will release implementing regulations or other guidance materials before September 1, 2021, when the law takes effect. As a point of reference, the Chinese government has not issued additional guidance on the International Criminal Judicial Assistance Law, which prohibits, among other things, unauthorized cooperation of a broad nature with foreign criminal authorities, since the law was passed in 2018. Nevertheless, given that data security and privacy are one of Beijing's areas of focus, it is possible that the Chinese government will issue regulations, statutory interpretation, or guidance to clarify certain key requirements in the Data Security Law.

Personal Information Protection Law of the People's Republic of China

On April 29, 2021, China released the second draft of its Personal Information Protection Law, which seeks to create a legal framework similar to the European Union's General Data Protection Regulations ("GDPR"). The draft Personal Information Protection Law, if passed, will apply to "personal information processing entities ("PIPEs")," defined as "an organization or individual that independently determines the purposes and means for processing of personal information."[11] The draft Personal Information Protection Law defines processing as "the collection, storage, use, refining, transmission, provision, or public disclosure of personal information."[12] The draft Personal Information Protection Law also defines "personal information" broadly as "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person," but excludes anonymized information.[13]

The draft Personal Information Protection Law requires PIPEs that process certain volumes of personal data to adopt protective measures, such as designating a personal information protection officer responsible for supervising the processing of applicable data.[14] PIPEs also would be required to carry out risk assessments prior to certain personal information processing and conduct regular audits.[15]

Under Article 38 of the draft Personal Information Protection Law, the Cyberspace Administration of China ("CAC") will provide a standard contract for PIPEs to reference when entering into contracts with data recipients outside of China. The draft Personal Information Protection Law provides that PIPEs may only transfer personal information overseas if the PIPE: (1) passes a security assessment administered by the CAC; (2) obtains certification from professional institutions in accordance with the rules of the CAC; (3) enters into a transfer agreement with the transferee using the standard contract published by the CAC; or (4) adheres to other conditions set forth by law, administrative regulations, or the CAC.[16] Like the Data Security Law, the draft Personal Information Protection Law does not elaborate on this requirement, including what types of certifications would satisfy the requirement under Article 38 or what "other conditions set forth by law, administrative regulations, or the CAC" entail.

Similar to Article 36 of the Data Security Law, Article 41 of the draft Personal Information Protection Law prohibits providing personal data to judicial or law enforcement bodies outside of China without prior approval of competent Chinese authorities.[17] As with the Data Security Law, neither the "competent Chinese authority" nor the approval process is

further defined, however.

The draft Personal Information Protection Law does not include penalties specifically tied to Article 41, but does set forth general penalty provisions in Article 65, which include confiscation of illegal gains, and a basic fine of up to 1 million CNY (approximately $156,000) for companies and between 10,000 CNY and 100,000 CNY (approximately $15,600 to $156,000) for responsible persons.[18] "Severe violations," which the statute does not define, may be punishable by a fine up to 50 million CNY (approximately $7.8 million) or up to five percent of the company's annual revenue for the prior financial year, as well as fines between 100,000 CNY to 1 million CNY (approximately $156,000 to $1.56 million) for responsible persons. Additionally, companies found to have violated the Personal Information Protection Law may be subject to revocation of business permits or suspension of business activities entirely.

The Data Security Law and Personal Information Protection Law in Context

The Data Security Law and, if enacted, the Personal Information Protection Law add to a growing list of Chinese laws that restrict the provision of data to foreign governments. For example:

- The **International Criminal Judicial Assistance Law** bars entities and individuals in China from providing foreign enforcement authorities with evidence, materials, or assistance in connection with criminal cases without the consent of the Chinese government.[19]
- Article 177 of the **China Securities Law** (2019 Revision), prohibits "foreign regulators from directly conducting investigations and collecting evidence" in China and restricts Chinese companies from transferring documents related to their securities activities outside of China unless they obtain prior approval from the China Securities Regulatory Commission.
- The newly released draft amendment to China's **Anti-Money Laundering Law** contains disclosure and pre-approval requirements for Chinese companies responding to data requests by foreign regulators.
- As Gibson Dunn has previously covered, the **Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures**, issued by the Ministry of Commerce of the PRC in January 2021, established a mechanism for the government to designate specific foreign laws as "unjustified extraterritorial applications," and subsequently issue prohibitions against compliance with these foreign laws.

The Data Security Law and draft Personal Information Protection Law, however, appear to surpass these prior prohibitions in several key respects. In contrast to the International Criminal Judicial Assistance Law, for example, the Data Security Law and draft Personal Information Protection Law do not require the data to be provided in the context of a criminal investigation for the transfer prohibitions to apply. The new restrictions ostensibly apply to data transfers in connection with a civil enforcement action or investigation, such as those conducted by the U.S. Securities and Exchange Commission. (They might also create yet another impediment to the provision of audit work papers by China-based accounting firms to the SEC and the Public Company Accounting Oversight Board.) As written, the Data Security Law and draft Personal Information Protection Law prohibitions also would also apply to Chinese parties in civil litigation before foreign courts that may need to submit evidence in connection with ongoing cases. In fact, the current language could be read to prohibit non-Chinese citizens residing in China from providing information about themselves to their own government regulators, so long as the data is "stored in China." The Data Security Law does not explain when data is "stored in China," or how to address potential scenarios in which entities or individuals may have a legal obligation to submit information to foreign judicial or law enforcement authorities.

The Data Security Law, draft Personal Information Protection Law and earlier laws restricting data transfers create a great deal of uncertainty for companies operating in China. Because these laws do not specify the process for obtaining government approvals, the criteria for approval, or the responsible government agency, it has become increasingly difficult for companies to determine how to respond to foreign regulators' demands to produce data that may be stored in China, conduct internal investigations in China in the context of an ongoing enforcement action or foreign government investigation, or comply with disclosure and cooperation obligations under various forms of settlement agreements with foreign authorities such as deferred prosecution agreements. Companies considering self-reporting potential legal violations in China to their foreign regulators, as well as cooperating in ensuing investigations conducted by those regulators, also will need to consider whether any of the relevant data was previously "stored in China," and if so, whether they are permitted to submit such data to foreign authorities without approval by Chinese authorities. The new statutes also raise concerns for professional services organizations, such as law firms, accounting and forensic firms, litigation experts, and others whose work product may reflect data that was "stored in China." The new laws do not make clear how they might apply to work product that is simply based on, reflects or incorporates data stored in China, and whether professional services firms are required to seek approval from relevant Chinese authorities before sharing such work product in foreign judicial proceedings or with enforcement authorities.

Gibson Dunn will continue to closely monitor these developments, as should companies operating in China, in order to minimize the risks associated with being caught in the vice of inconsistent legal obligations.

---

[1] Please note that the discussions of Chinese law in this publication are advisory only.

[2] Data Security Law, Art. 1 and 2.

[3] Data Security Law, Art. 27, 29, 30.

[4] Data Security Law, Art. 45

[5] Data Security Law, Art. 45.

[6] Data Security Law, Art. 45.

[7] Data Security Law, Art. 21.

[8] Data Security Law, Art. 36.

[9] Data Security Law, Art. 48.

[10] Data Security Law, Art. 21.

[11] Draft Personal Information Protection Law Art. 4, 72.

[12] Draft Personal Information Protection Law, Art. 4.

[13] *Ibid.*

[14] Draft Personal Information Protection Law, Art. 52.

[15] Draft Personal Information Protection Law, Art. 54, 55.

[16] Draft Personal Information Protection Law, Art. 38

[17] Draft Personal Information Protection Law, Art. 41.

[18] Draft Personal Information Protection Law, Art. 65.

[19] International Criminal Judicial Assistance Law, Art. 4.

The following Gibson Dunn lawyers assisted in preparing this client update: Patrick F. Stokes, Oliver Welch, Nicole Lee, Ning Ning, Kelly S. Austin, Judith Alison Lee, Adam M. Smith, John D.W. Partridge, F. Joseph Warin, Joel M. Cohen, Ryan T. Bergsieker, Stephanie Brooker, John W.F. Chesley, Connell O'Neill, Richard Roeder, Michael Scanlon, Benno Schwarz, Alexander H. Southwell, and Michael Walther.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's Anti-Corruption and FCPA, White Collar Defense and Investigations, International Trade, and Privacy, Cybersecurity and Data Innovation practice groups:

Asia:
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Oliver D. Welch – Hong Kong (+852 2214 3716, owelch@gibsondunn.com)

Europe:
Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Richard W. Roeder – Munich (+49 89 189 33-160, rroeder@gibsondunn.com)

United States:
Judith Alison Lee – Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Stephanie Brooker – Washington, D.C. (+1 202-887-3502, sbrooker@gibsondunn.com)
John W.F. Chesley – Washington, D.C. (+1 202-887-3788, jchesley@gibsondunn.com)
Joel M. Cohen – New York (+1 212-351-2664, jcohen@gibsondunn.com)
John D.W. Partridge – Denver (+1 303-298-5931, jpartridge@gibsondunn.com)
Michael J. Scanlon – Washington, D.C. (+1 202-887-3668, mscanlon@gibsondunn.com)
Adam M. Smith – Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com)
Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Patrick F. Stokes – Washington, D.C. (+1 202-955-8504, pstokes@gibsondunn.com)
F. Joseph Warin – Washington, D.C. (+1 202-887-3609, fwarin@gibsondunn.com)

Related Capabilities

Anti-Corruption & FCPA

White Collar Defense and Investigations

International Trade

Privacy, Cybersecurity, and Data Innovation

Accounting Firm Advisory and Defense