Legal Commentary

July 29, 2021

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

The Next Stage of Data Export Compliance

Authors: David TANG | Michelle GON | Chen MA

China has recently taken a series of actions to safeguard data security, particularly with respect to cross-border transfers of sensitive data. These actions include the following.

- **June 10**. The NPC Standing Committee adopted the *Data Security Law of the People's Republic of China*[1] (the "**Data Security Law**"), which will provide greater clarity for cross-border data transfer requirements and, among others, strengthen oversight of data provided to foreign law enforcement and judicial authorities.
- **July 6**. The Chinese cyberspace authority issued a take-down order of Didi apps from domestic app stores over data security concerns, following the company's high-profile U.S. public listing. Chinese authorities have since commenced a cybersecurity review of Didi's operations.
- **July 6**. The central government issued important policymaking opinions that call for capital market reforms, including increased supervision of overseas-listed companies, enhancement of related data security matters, and increased intergovernmental cooperation, among others.
- **July 10**. The Chinese cyberspace authority issued an exposure draft of proposed revisions to the *Measures for Cybersecurity Review*, which highlights the authority's position toward enhancing reviews of data security requirements in China, notably with respect to large-scale data processing activities and foreign public listings of certain Chinese companies.

These developments in part reflect the clear intent of the Chinese government to restrict sensitive data flows between China and foreign jurisdictions and their government authorities. In this article, we provide highlights of these developments as they relate to cross-border data transfer compliance. We then provide our insights and recommendations as we move toward the next stage of cross-border data transfer compliance in China.

Precursors: Cybersecurity Law and piecemeal approach to cross-border transfer restrictions and approvals

[1] 《中华人民共和国数据安全法》 [Data Security Law of the People's Republic of China] (29 Standing Comm. 13 Nat'l People's Cong., P.O. 84; adopted June 10, 2021, effective Sept. 1, 2021).

Restrictions in China on cross-border data flows are not new. The *Cybersecurity Law of the People's Republic of China*[2] (the "**Cybersecurity Law**") formally imposed in 2017 certain data localization and cross-border transfer requirements. The Cybersecurity Law at Article 37 requires localization and cross-border transfer assessments for operators of critical information infrastructure ("**CII operators**") that intend to transfer cross-border either personal information or so-called "important data". As many readers will attest, the compliance environment for CII operators and cross-border data transfers under the Cybersecurity Law has continued to be murky, despite a series of proposed rulemakings intended to better define these requirements.

Following the Cybersecurity Law, other laws have restricted cross-border data transfers of certain types of data and in specified instances. Competent authority approval is generally required under these circumstances.

- **Foreign authority investigations and data transfers**. Restrictions were imposed for evidence gathering by, and cooperation with, foreign authorities in China in the context of civil matters (2017)[3] and criminal matters (2018)[4,5]. These legal developments generally reiterate the need for parties to adhere to protocols of existing treaties or to obtain Chinese competent authority approval before cooperating with foreign authorities in evidence gathering and related activities. Similar legal provisions have been adopted specifically in the context of foreign securities regulatory investigative activities (2020)[6].
- **Industry-specific data transfer restrictions**. Competent authority approval is required by law for cross-border transfers of certain types of sensitive data. For example, genetic materials are now subject to strict limitations and approval requirements for cross-border transfer, such as for use in clinical trials[7].

Highlights of recent developments

I Data Security Law

In this regard, we observe the Data Security Law assists in better classifying types of sensitive data, reiterates general cross-border data transfer requirements, and imposes broader oversight of data to

[2] 《中国人民共和网络安全法》 [Cybersecurity Law of the People's Republic of China] (24 Standing Comm. 12 Nat'l People's Cong., P.O. 53; adopted Nov. 7, 2016, effective June 1, 2017).

[3] 《中华人民共和国民事诉讼法》 [Civil Procedure Law of the People's Republic of China] art. 277 (restricting foreign civil investigative activities) (*as amended by* 28 Standing Comm. 12 Nat'l People's Cong., P.O. 71; adopted June 27, 2017, effective July 1, 2017).

[4] For further insights, see *A Look at China's New Criminal Judicial Assistance Law* (Han Kun Law Offices, Nov. 22, 2018).

[5] 《中华人民共和国国际刑事司法协助法》 [Law of the People's Republic of China on International Judicial Assistance in Criminal Matters] art. 4 (requiring competent authority approval to assist in foreign criminal investigations) (6 Standing Comm. 13 Nat'l People's Cong., P.O. 13; adopted and effective Oct. 26, 2018).

[6] 《中华人民共和国证券法》 [Securities Law of the People's Republic of China] art. 177 (restricting foreign securities investigative activities) (*as revised by* 15 Standing Comm. 13 Nat'l People's Cong., P.O. 37; adopted Dec. 28, 2019, effective Mar. 1, 2020).

[7] 《中华人民共和国生物安全法》 [Biosecurity Law of the People's Republic of China] art. 56 et seq. (imposing restrictions on cross-border transfer of genetic materials) (22 Standing Comm. 13 Nat'l People's Cong., P.O. 56; adopted Oct. 17, 2020, effective Apr. 15, 2021).

be transferred to foreign law enforcement and judicial authorities. We address each of these in turn.

- **Data classification.** The Data Security Law calls for important data classification catalogues to be developed by each industry competent authority. In addition, the law introduces a new type of data, "core state data", which will be subject to stricter oversight and is defined as "data that are related to national security, lifelines of the national economy, and are important to people's livelihoods and major public interests." Cross-border data transfer restrictions will no longer be based on the transferor's designation as a CII operator, but rather based on the nature and importance of the data.

- **Clarity for transfer requirements.** The Data Security Law reiterates that CII operators must follow the Article 37 requirements of the Cybersecurity Law, while empowering the Chinese cyberspace and other authorities to formulate separate rules for other data processors. We expect these provisions to allow the authorities to provide further clarity for business operators in China to comply with Article 37.

- **Restrictions as to foreign law enforcement authorities.** The Data Security Law stipulates that, absent an applicable treaty, intergovernmental agreement, or reciprocity, the Chinese competent authorities must approve *any* transfer of data in China to foreign law enforcement and judicial authorities. This blanket approval requirement adds clarity to the previous piecemeal approach adopted in prior legislation.

II Policymaking opinions and Revision Draft to the Measures for Cybersecurity Review

1. Policymaking opinions

On July 6, 2021, central policymakers issued important opinions on reforming China's capital markets, *Opinions on Strictly Cracking Down on Illegal Securities Activities in Accordance with the Law*[8] (the "**Opinions**"). The Opinions call for enhancing law enforcement in China's capital markets and set certain goals in this regard to be achieved by 2025. In relevant part, we observe that the Opinions call for (i) strengthening cross-border regulatory and judicial cooperation and enforcement; and (ii) improving laws and regulations in respect of data security, cross-border data flows, and the management of confidential information.

2. Proposed revisions to the Measures for Cybersecurity Review

China's cyberspace authority issued on July 10, 2021 an exposure draft[9] of proposed revisions to the *Measures for Cybersecurity Review*[10] (the "**Measures**"; the "**Revision Draft**"). The Measures presently require a cybersecurity review process for the procurement activities of CII operators that

[8] 《关于依法从严打击证券违法活动的意见》 [Opinions on Strictly Cracking Down on Illegal Securities Activities in Accordance with the Law] (Gen. Office Cent. Comm. CPC, Gen. Office St. Council; promulgated July 6, 2021).

[9] 《关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知》 [Circular on Seeking Public Comments for the Measures for Cybersecurity Review (Revision Draft for Comment)] (Cyberspace Admin. China; issued July 10, 2021 for public comment until July 25, 2021).

[10] 《网络安全审查办法》 [Measures for Cybersecurity Review] (Cyberspace Admin. China et al, Decr. 6; promulgated Apr. 13, 2020, effective June 1, 2020).

could affect national security. However, the Revision Draft would:

A. Expand the scope of cybersecurity reviews to include:

- Data processors whose data processing activities could affect national security; and
- Foreign listings of CII operators and data processors that hold the personal information of more than 1 million individuals.

B. Consider in cybersecurity reviews procurement activities, data processing activities, and foreign listings that:

- Could risk core data, important data, or a large amount of personal information being stolen, leaked, destroyed, and illegally used or exiting China; and
- Could risk CII, core data, important data, or a large amount of personal information being influenced, controlled, or maliciously used by foreign governments after listing in foreign countries.

The Revision Draft would adapt the Measures to realize relevant provisions of the Data Security Law and the Opinions by mandating competent authority review and approval for potential cross-border transfers of personal information and important data by CII operators and data processors in the context of foreign listings.

Han Kun's observations

Taken as a whole, we believe the Data Security Law may have finally ended the years-long wait for an expected step up in administrative rulemaking and enforcement activity around cross-border data transfers. We have the following observations at the current juncture.

I The Data Security Law provides a clearer roadmap for administrative rulemaking around data classification and cross-border transfer requirements

Upon adoption of the Data Security Law, we now see the following important highlights for data classification.

- **Core state data**. Core state data will presumably be prohibited from transfer cross-border, although the scope of core state data is to be further clarified by administrative rules and/or national standards.
- **Important data and personal information (CII operators)**. The Data Security Law reiterates the Cybersecurity Law Article 37 requirements, we expect localization and competent authority approval for cross-border transfers of personal information and important data.
- **Important data and personal information (network operators).** Other network operators will be subject to to-be-formulated administrative rules that we expect will be more relaxed in scope.
- **Provision of data to foreign authorities.** As opposed to the former piecemeal approach, Chinese lawmakers have taken a clear position on the provision of data to foreign law enforcement

and judicial authorities – no provision without approval, absent an applicable treaty, intergovernmental agreement or reciprocity.

The Data Security Law provides an important milestone for advancing administrative rulemaking in respect of cross-border transfers. Already, the Revision Draft clearly contemplates the cross-border transfer of important data and personal information when it proposes a cybersecurity review for foreign listings of CII operators and other companies that hold such data. We expect more rulemaking on cross-border data transfers to be forthcoming.

II "Foreign law enforcement authority" to be broadly defined, presumed to include foreign securities authorities

The Data Security Law, by its language, will apply to all provisions of data to foreign law enforcement and judicial authorities. This will include evidence gathering and information requests for foreign criminal proceedings, civil proceedings, and administrative investigations. We believe the term "**foreign** law enforcement authority" should be viewed broadly, including foreign securities and other authorities. This is reflected in the Opinions, which envision greater intergovernmental cooperation with foreign jurisdictions in respect of capital markets.

III Emphasis on treaties and intergovernmental agreements, uncertainty around other foreign authority data transfers

Intergovernmental agreements currently exist for the cross-border transfer of data. For example, a joint regulatory cooperation memorandum exists between the U.S. securities authority, the Securities and Exchange Commission, and its Chinese counterpart regarding the production of evidence in connection with foreign securities litigation and investigative proceedings. In this case, once the Data Security Law takes effect, we believe evidence production to the U.S. securities authority will more or less follow the same protocol; except that the necessary requirements under the Data Security Law must be followed with respect to "important data" and "core state data", for which the Revision Draft provides a prelude.

It remains unclear how the Data Security Law will apply to other foreign proceedings that are not subject to an existing treaty or intergovernmental agreement, such as cartel investigations, consumer protection class actions, and ordinary commercial litigation. Based on the Data Security Law, as long as the data receiver is a foreign law enforcement or judicial authority, approval by a Chinese competent authority will be required.

IV Business operators in sensitive industries must be mindful

Business operators in sensitive industries that intend to transfer data cross-border may be subject to industry-specific legal requirements. These include operators in the biotechnology and life sciences industries. It is necessary to identify and observe these industry-specific requirements when structuring business arrangements.

V Enforcement has begun, compliance cannot be an afterthought

We believe the recent Didi app take-down order and cybersecurity review actions to represent a

milestone case of enforcement vis-à-vis cross-border data transfers. Viewed as such, these actions set the tone for future enforcement and compliance activities. The future is now to comply with cross-border data transfer requirements.

Recommendations

The restrictions on cross-border data transfers have been long awaited. As we discuss, we expect administrative rulemaking to provide further guidance in this area soon, with the Revision Draft being only the first of many such developments. In this respect, we recommend business operators to take the following actions.

- Data classification will be critical. Create internal controls that classify data types and establish protocols for cross-border transfers.
- Allocate more resources to cross-border transfer compliance. Besides a general increase in enforcement activities, we anticipate cross-border transfer reviews and assessments may serve as a tool to counter foreign sanctions and advance policy interests.
- Consult with counsel before completing cross-border transfers of data to foreign law enforcement or judicial authorities to determine the applicable approval requirements.
- Continue to monitor administrative rulemaking and standard setting in this area to ensure continued compliance with the Data Security Law and other applicable provisions.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

David TANG

Tel: +86 21 6080 0905
Email: david.tang@hankunlaw.com

Michelle GON

Tel: +86 21 6080 0559
Email: michelle.gon@hankunlaw.com

Chen MA

Tel: +86 10 8525 5552
Email: chen.ma@hankunlaw.com