

Legal Commentary

November 7, 2023

A First Look at the Provisions on Regulating and Promoting Cross-border Data Flows (Draft for Comment)

Authors: Kevin DUAN | Yuting WANG | Minzhe HU | Yi ZOU

Introduction

On September 28, 2023, the Cyberspace Administration of China (the “**CAC**”) issued the *Provisions on Regulating and Promoting Cross-border Data Flows (Draft for Comment)* (the “**Draft Provisions**”). In light of the previous practical issues relating to data export security assessments, standards for PI exports, and contract record-filing, the Draft Provisions would significantly adjust the applicable standards for data export assessment and record-filing and substantially exempt enterprises from the evaluation and record-filing obligations for scenarios where data exports are necessary or where only a small amount of PI is to be transferred. While ensuring the orderly cross-border transfer of data, enterprises’ compliance burdens would be substantially reduced. Under the background of downward pressure on the overall economy, the Draft Provisions offer more certainty and possibility for data to be exported, which substantially responds to the Chinese government’s initiative of adhering to economic globalization under the new situation and provides the source driving force for enterprise development.

Notably, the Draft Provisions do not waive the basic requirements for data security and PI protection under the Data Security Law, the PI Protection Law, and other relevant laws and regulations. Even for enterprises which would be exempted from data export assessment and standard contract filing under the Draft Provisions, it remains necessary to ensure compliance in data export activities by entering into a data transfer agreement and conducting an assessment of the impact of PI protection related to the export of data and other basic data compliance systems to avoid interim and ex post regulatory risks in respect of data export activities.

This article provides an overview of the Draft Provisions based on the above background.

Basic principles

There are 11 articles in total in the Draft Provisions, which reflect the following basic regulatory principles.

- **Whitelist system:** Articles 1 to 4 of the Draft Provisions specify the type of data transmission, the source of data transmission, and the scenarios of cross-border data transmission for which enterprises may be exempted from undergoing a data export security assessment, entering into and

filing a standard contract, or undergoing a PI protection certification.

- **Expected quantity of data exports is the only consideration:** Articles 5 and 6 of the Draft Provisions propose new quantitative standards to determine whether it is necessary to file a data export security assessment, enter into a standard PI cross-border transfer contract, or undergo PI protection certification. This quantitative standard considers only the quantity of PI to be exported in one year; it does not consider the quantity of PI a PI handler actually possesses or the quantity of PI that has been exported.
- **Three levels of compliance obligations:** Articles 5 and 6 of the Draft Provisions provide three levels of compliance obligations for thresholds between the number of individuals whose PI is to be exported within one year. Specifically, if the number of individuals is one million or more, the parties concerned must apply for a data export security assessment; if the number of individuals is 10,000 or more but fewer than one million, the parties concerned must enter into standard contracts for PI cross-border transfer (“Standard Contracts”) or undergo PI protection certification; if the number of individuals is less than 10,000, the parties concerned do not need to apply for data export security assessment, enter into a standard contract, or undergo PI protection certification.
- **Exceptions for free trade zones (“FTZs”):** On the basis of the whitelist system, Article 7 of the Draft Provisions would further relax the rules on cross-border data transfers within China’s FTZs by authorizing each FTZ to establish a negative list system similar to foreign investment restrictions. FTZs could formulate, on their own, lists of data to be included in the scope of data export security assessment, standard contract, and PI protection certification and administration. Apart from this, no relevant obligations would be required to be performed to export data.

It should be noted that, although the Draft Provisions would greatly reduce the requirements for security assessment or record-filing for data exports, increasing the flexibility of the system, it also considers security issues relating to data exports. At the same time, the Provisions propose new measures to strengthen interim and ex post supervision of data exports. This suggests that enterprises still need to pay great attention to the security and compliance of data exports and to adjust their compliance measures in a timely manner based on specific changes in data export activities.

Specific rule changes

I. Whitelist system

A common problem in the existing rules on data export assessment and record-filing is the uncertainty created by a lack of clear assessment criteria. In particular, there is a wide gap between the perspectives of enterprises and regulators in judging the necessity of data exports. In addition, companies are at a loss as to whether the export of data involves important data, which has always been vaguely defined, and whether it triggers a data export security assessment. Therefore, many enterprises are hesitant on the issue of what data can be exported, which has brought obstacles to actual enterprise operations.

With regard to this issue, the Draft Provisions would generally establish whitelist rules and enumerate

issues such as scenarios for data exports that do not require a security assessment or record-filing, the conditions under which important data will trigger the security assessment, etc., which would, to a large extent, resolve the above-mentioned pain points. In particular, the exemption for highly necessary and common scenarios and those with low potential security risks (such as those for the performance of contracts involving foreign elements and those for internal human resources management of multinational corporations) would significantly reduce the burden on enterprises and avoids the creation of additional obstacles to ordinary foreign-related economic and trade activities and operations and management.

1. Exemption for inbound and outbound data export scenarios

Article 3 of the Draft Provisions clarifies that no data export security assessment or record-filing of a standard contract is required for the export of PI collected outside of the PRC. This provision is consistent with the previous regulatory approach. According to Article 3.7 of *Information Security Technology — Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comment)*, “[i]f the PI and important data not collected or generated from domestic operations pass through that country without any modification or processing, the cross-border transfer of data shall not be regarded as cross-border transfer of data” and “[i]f the PI and important data not collected or generated from domestic operations are to be stored or processed within the territory, the cross-border transfer of data shall not be regarded as cross-border transfer of data if it does not involve the PI and important data collected or generated from domestic operations.”

With the wave of data exports, more and more Chinese enterprises are conducting operations all over the world, and some of them even specialize in overseas markets and have no actual operations in China. It is also possible that the Chinese entity of a multinational corporation (“MNC”) undertakes some PI processing responsibilities on a global basis. For the purposes of unified management, cost control, and industrial chain division, PI of overseas entities generated in overseas operations may be transmitted back to China and processed by domestic entities. Typically, a PRC enterprise provides customer service, logistics, cloud storage, data analysis, or other support services for overseas businesses. In such cases, the PI collected from overseas is then processed in China and exported. We understand that Article 3 of the Draft Provisions is intended to make clear that this entry and re-exit scenario does not fall within the scope of the data export rules, which would eliminate the previous regulatory uncertainty on this issue. This is undoubtedly of great benefit to both PRC enterprises carrying out overseas operations and MNC enterprises carrying out divisions of labor globally.

2. Exemptions in specific scenarios

Contract performance: Article 4 (1) of the Draft Provisions first excludes scenarios in which PI must be exported for the purpose of entering into and performing a contract to which an individual is a party (e.g., cross-border shopping, cross-border remittance, airline tickets and hotel reservations, visa processing, etc.). This article provides a non-exhaustive guide for “necessary for the performance of a contract” through common real-life scenarios. For MNCs, their R&D, production, sales, and other business environments may not be possible without collaborations among different entities around the world. On the other hand, this paragraph provides more room for enterprises to organize business

activities in a reasonable and efficient manner, so as to avoid the adverse effects on business operations caused by excessive compliance costs in exit scenarios.

HR scenarios: PI of an employer's employees may be exported without prior approval in scenarios where it is necessary for human resources management which is implemented either in accordance with the employer's lawfully formulated rules or lawfully executed collective contracts. Therefore, the Draft Provisions provides for exemption of PI to be exported in HR scenarios, which is also the daily management practice of many MNCs. MNCs would no longer need to consider the situations in which the PI of their employees is exported when arranging their PI export scenarios. This article should be interpreted strictly. For example, job seekers who have not signed an employment agreement with a prospective employer would not fall under the HR management scenario exemption.

Emergency scenarios: No prior approval would be required in emergency situations where it is necessary to export PI to protect the life, health, and property security of natural persons. In emergency situations, both obtaining the consent of PI subjects and the prior approval for PI export both have practical barriers and are not in line with the original intention of the PI Protection Law. Therefore, the Draft Provisions take this practice into full consideration and show respect for and protection of the rights and interests of PI subjects.

II. PI export compliance measures linked only to the amount of PI exported

The Draft Provisions propose the following adjustments to address issues with respect to the existing data export regime, such as the triggering of security assessment and the calculation of the data threshold for the filing of standard contracts. The proposed rules are clearer, easier to understand, and more practical and eliminate unreasonable circumstances where disproportionate compliance requirements are imposed on a small amount of data with low apparent risk.

The amount of PI entities possess no longer considered: Unlike the *Measures on Security Assessment for Data Cross-border Transfers*, the Draft Provisions do not set any threshold for the amount of PI a PI handler processes. In practice, it is possible that a PI handler may process the PI of more than one million individuals within China but the amount of this PI that is exported is actually quite limited. In this instance, high compliance costs would be imposed if a security assessment were conducted in strict accordance with the *Measures on Security Assessment for Data Cross-border Transfers*, and it is likely that those costs would not be commensurate with the actual data export risks. To avoid such situations, the Draft Provisions would no longer consider domestic PI which PI handlers possess and directly regulate the amount of PI to be exported.

The period to calculate the amount of data exported reduced from two years to one year: The Draft Provisions propose examining the estimated amount of PI to be exported when determining relevant PI export obligations. This is in contrast to the *Measures on Security Assessment for Data Cross-border Transfers* and the *Measures on Standard Contracts for PI Cross-border Transfers*, which focus on the overall amount of data processed by an enterprise and the amount of PI exported since January 1 of the previous year. Notably, Article 11 of the Draft Provisions clearly provides that they would prevail over other relevant administrative rules in the case of any inconsistency, including the *Measures on Security Assessment for Data Cross-border Transfers* and the *Measures on Standard*

Contracts for PI Cross-border Transfers. Thus, under the Draft Provisions, if an enterprise wished to qualify for an export exemption or reduce its obligations, it would need to focus on estimating the amount of PI that will be exported in the following year.

Clarifying the lower limit for the PI of 10,000 individuals: In terms of the amount of PI to be exported, another major change in the Draft Provisions is that if the PI to be exported in one year relates to 10,000 individuals or fewer, the pre-approval formalities for data exports would not be required, which is in contrast to the current situation which calls for the signing and filing of a standard contract for any PI exports. Therefore, Article 5 of the Draft Provisions would greatly reduce the operating burden and facilitate the development of cross-border activity for small and medium-sized enterprises and those with simple export scenarios and a low overall volume of PI exports.

No distinction between general PI and sensitive PI: Notably, the Draft Provisions do not contain stipulations with respect to sensitive PI; instead, Article 8 provides that sensitive PI is to be exported in accordance with the relevant laws, administrative regulations, and departmental rules. Article 11 of the Draft Provisions also provides that “if there is any inconsistency between the Measures on Security Assessment for Data Cross-border Transfers, the Measures on Standard Contracts for PI Cross-border Transfers and other relevant regulations and the [Draft Provisions], the [Draft Provisions] shall prevail”, we understand that if the Draft Provisions are promulgated in their current form and no other laws, regulations or departmental rules apply, the strict calculation standards for sensitive PI for export will be significantly weakened.

III. Special FTZ rules

The Draft Provisions are the first to propose a negative list regime for data exports. Article 7 of the Draft Provisions provides that “Free Trade Zones may formulate their own lists of data to be included in the scope of data export security assessment, standard contracts, and PI protection certification (“**Negative List**”) in the Free Trade Zone. Such lists shall be filed with the national cyberspace administration authority for the record after being approved by the cyberspace administration commission at the provincial level. For data not included in the Negative List, parties are not required to file a data export security assessment, enter into a standard contract for PI to be exported, and go through PI protection certification.” By contrast, the “whitelist” exempts exports under certain scenarios or of less than a specified volume, while the “negative list” only retains regulation on a small amount of data while relaxing requirements on other data exports. In other words, allowing the FTZs to establish a “negative list” in effect, would allow the FTZs to explore a more relaxed regulatory policy.

The FTZs would be allowed to explore a negative list system not only due to their positioning in China’s economic development, but also based on practical industrial development. Located within mainland China but outside customs, the FTZs have special preferential policies in industrial and commercial registration, enterprise tax, foreign investment, and talent introduction, which have broken through the policy restrictions imposed by China’s customs to some extent. In particular, in response to the relatively urgent and diversified data export needs of enterprises in the FTZs, the FTZs may, while regulating security, focus more on development and promote the cross-border data flows. In addition, institutional innovation in the FTZs also promotes the implementation of the relevant national-level

regulatory systems, while enhancing the operability and enforceability of the existing laws and regulations.

In this context, there are precedents in the FTZs to explore innovative data export regulations. For example, Article 33 of the *Regulations on Lin-gang Special Area of China (Shanghai) Pilot Free Trade Zone* provides that “pursuant to the relevant laws and regulations of the State, Lin-gang Special Area shall explore the development of a low-risk cross-border flow data catalogue, so as to promote safe and orderly cross-border flow of data.” The *Opinions of Shenzhen on Several Special Measures for Relaxing Market Access for the Building of a Socialist Demonstration Zone with Chinese Characteristics* call for carrying out pilot projects for cross-border data transmission (export) security management under the framework of the national and industry data cross-border transmission security management system and establishing data security management mechanisms such as data security protection capacity evaluation and certification, data circulation backup and examination, cross-border data circulation, and transaction risk evaluation, etc.

Given that the current regulatory system for data exports has been preliminarily established, it is timely and operable at the regulatory level for the FTZs to further explore opening up the data export policies. As some FTZs (ports) in China already have relatively complete industrial ecologies and market application foundations, the local regulatory authorities of the FTZs may conduct field investigations and research in relevant industries and business areas where they have comparative advantages (such as biomedicine and social media sectors in Beijing, and the finance, automobile and industrial internet sectors in Shanghai FTZ), understand the business situations of relevant industries, listen to expert advice, and prepare a list of data prohibited to be exported, which provides an important reference for the regulation on the data exports from other regions.

Impact on existing data export security assessments and filing of standard contracts

The Draft Provisions would significantly revise the current data export assessment and record-filing rules established in the relevant provisions, including the *Measures on the Security Assessment on Cross-border Data and the Measures on Standard Contracts for Cross-border Data Transfer of PI*, and expressly provide that these new provisions will supersede such existing rules once they come into effect. Such substantive changes would have a significant impact on enterprises that have already submitted or are preparing for data export security assessments and standard contracts. Although the Draft Provisions are still at the consultation stage, given the background of its introduction and the relevant time limits under the existing data export regulations, we have reason to believe that it will be formally promulgated in the near future, in which case it will have a certain impact on enterprise data export compliance.

I. Impact on data export security assessments

1. Applications under examination

Enterprises that have already submitted the data export security assessments but who have not yet received a formal decision, or are still in the process of revising their application materials to comply with regulatory requirements, should reconsider the applicability of the data export security assessment based on the relevant scenario and consider the data export scenario in accordance with

the Draft Provisions. For scenarios in which data export security assessments would no longer be applicable pursuant to the Draft Provisions, it is recommended that enterprises communicate with the relevant regulatory authorities to discuss the possibility and methods to adjust and simplify existing applications. Given that most enterprises' data export declarations are still under review, we do not exclude the possibility that the regulatory authorities will provide a unified explanation on how to handle the above situations during the subsequent review of such applications.

2. Rectification in export scenarios already requested by regulatory authorities

For enterprises that have submitted data export security assessments and received rectification instructions regarding relevant data export scenarios, we recommend these enterprises communicate with the relevant regulatory authorities to clarify how the authorities should handle such applications and the assessment results if the relevant scenarios for their data export would no longer be subject to assessment based on the Draft Provisions. Nevertheless, given that the regulatory authorities have identified problems in data export through the filing documents submitted by the enterprise, the enterprise should continue to implement the rectification requirements and keep in close communication with the regulatory authorities in this regard.

II. Impact on filing of standard contracts

As for the filing of standard contracts, given that the implementation of the data export security assessment policy is late, the acceptance window for data export only officially opened on June 1, and most enterprises are still preparing for or evaluating relevant filing procedures. These enterprises should re-analyze the applicability of filing standard contracts to the scenarios in which their PI is to be exported and consider excluding those scenarios that would not be subject under the Draft Provisions. This is in view of the fact that the Draft Provisions specify minimum quantities of PI to be exported that are subject to the conclusion of a standard contract and the performance of filing procedures and other scenarios which are exempted.

Data export compliance: partial relaxation

The PI Protection Law, the Data Security Law, the Measures on Security Assessment for Data Cross-border Transfers, and other laws and regulations provide for three basic requirements of data export risk assessment, i.e. "legality, legitimacy, and necessity". The Draft Provisions would simplify the relevant administrative approval procedures for data export and reduce the compliance costs and operating burden of enterprises. In particular, from the perspective of "necessity", it will give enterprises more leeway to make judgments at their own discretion, fully recognize the business needs of enterprises' cross-border operation, and respond to the PRC government's initiatives on economic globalization.

However, this does not mean that the compliance standards for data export can be lowered. Whether a standard contract or data export security assessment is applicable to a data handler, the handler must ensure that it complies with the relevant statutory obligations. In respect of "legality", a typical example is the informed consent of PI subjects. The Draft Provisions, while clarifying that there is no need to apply for security assessment or to enter into a standard contract for certain export scenarios, still requires that "the consent of PI subjects shall be obtained when exporting PI on the basis of an individual's consent."

In respect of “security”, we focus on the impact on individual rights and interests and the security risks after data is exported. The Draft Provisions also reiterate that data handlers should “fulfill their data security and protection obligations to ensure the security of data to be exported”, and the regulatory authorities will continuously monitor the data export security incidents and security risks from interim and ex-post perspectives.

At this stage, enterprises may determine whether they still need to apply for data export security assessment or enter into a standard contract in light of the Draft Provisions:

- If the PI of 10,000 or fewer individuals is expected to be exported within one year, the Draft Provisions would not require an application for data export security assessment or entry into a standard contract. However, such enterprises still need to take the following measures to continuously protect the data export security and to consider the impact on the approval and filing procedures even after the Draft Provisions take effect.
- Enterprises will continue to sign data processing agreements or data transmission agreements with overseas data receivers, to specify the role of the overseas data receiver in data processing, and require the overseas data receiver to undertake that its processing meets the standards stipulated in China’s data protection laws and to take necessary measures to protect PI security.
- Enterprises will continue to make progress on PI protection impact assessments and prepare reports to demonstrate that they meet the exemption conditions in the Draft Provisions, demonstrate the necessity of their data exports, and prove that they have taken sufficient measures to protect data security in accordance with the law.
- Enterprises should continue to monitor the progress of the Draft Provisions and changes in enterprises’ data cross-border transmission activities, and decide whether to continue to apply for data export security assessment or to file a standard contract in accordance with the Draft Provisions, once the final version is promulgated.

For enterprises that expect to export PI of more than 10,000 individuals in one year but have a whitelist exemption scenario, they should assess the necessity of data export activities based on specific scenarios and assess the scale of their exports and decide on specific application strategies and subsequent export arrangements.

- If the enterprise’s data exports fall under a whitelist scenario, we understand that it is not necessary to apply for a security assessment or enter into a standard contract under that scenario. However, in this case, enterprises should prudently determine the scope of PI that must be exported. If an enterprise, at its own discretion, includes a field of PI that is obviously irrelevant to whitelisted scenarios into the scope of exemption from assessment and filing, it may face interim and ex post supervision by authorities.
- There may be different interpretations of the method to calculate the estimated exports under Articles 5 and 6 of the Draft Provisions. We tend to believe that PI in whitelisted scenarios will be excluded in the calculation of the estimated exports, and enterprises may calculate the estimated exports beyond whitelisted scenarios to decide whether to apply for a security assessment or enter into a standard

contract. We understand that this is in line with the basic principle to facilitate cross-border data flows established in the Draft Provisions, but the specific calculation method is still to be clarified by the authorities in the effective version of the Draft Provisions.

If some cross-border fields or scenarios are indeed absent, the exporter may also face practical obstacles in the subsequent security assessment for the declaration or the filing of the standard contract. In this case, we recommend companies explore the feasibility of data processing localization as soon as possible or avoid the export of unnecessary fields. Once the FTZs release of their data export negative lists, enterprises may consider carrying out data export activities in accordance with these special rules.

Conclusion

Filing for data export assessment, including data export security assessment and filing of standard contracts has been the focus of many enterprises' compliance efforts in the past year or so. Current data export rules focus on security assessment, which indirectly leads to situations in which the data to be exported is relatively small, the risk involved is relatively low, and the scenarios involving high necessity may also trigger a security assessment or filing. This, to some extent, imposes a compliance burden on some enterprises that is disproportionate to the actual risk of the data to be exported. In addition, in the actual review process, under the existing rules, there are wide gaps in judgment by enterprises and the regulatory authorities with respect to key factors such as the necessity of the export, and there are no reliable standards for whether specific scenes or fields may be used for exporting enterprises. In addition, the low certainty of such assessment rules also causes obstacles to the daily operation and business development of enterprises. Many enterprises' data export compliance work is caught in this dilemma.

The Draft Provisions, released on the eve of the Mid-Autumn Festival, would provide targeted solutions to these problems. As market players, we are happy to see the regulatory authorities adjust the current rules in a timely manner to alleviate enterprises' practical difficulties and reduce unnecessary burdens, provide safe and practical data export assessment and filing solutions, and provide the necessary bottom line for enterprises' global operations in a digitalized environment.

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:

Kevin DUAN

Tel: +86 10 8516 4123

Email: kevin.duan@hankunlaw.com