HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

April 13, 2017

Comments on the Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (for Public Comment)

David TANG | Min ZHU

On April 11, 2017, the Cyberspace Administration of China ("**CAC**") issued the *Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad* (for Public Comment) ("**Measures**"), seeking public comment. The Measures will act to support the *Cybersecurity Law of the People's Republic of China* ("**Cybersecurity Law**") which comes into effect on June 1, 2017. As one of the important supporting documents to the Cybersecurity Law, the Measures are intended to specifically implement the personal information and important data export security assessment requirements found in Article 37. Although the current Measures are only a draft for comment, much regulatory focus has been placed on the cross-border transfer of data.

Subject to supervision regardless of enterprise type

The Measures explicitly expand the scope of persons subject to data export security assessments.

Article 37 of the Cybersecurity Law provides that "personal information and important data generated or collected by operators of critical information infrastructure within the territory of the People's Republic of China shall be stored within China. If it is necessary to transmit data abroad due to business needs, security assessments shall be conducted in accordance with measures formulated by the CAC in conjunction with the relevant departments of the State Council." The Cybersecurity Law further provides that the scope of "critical information infrastructure" is limited to that which is described in Article 31, namely "important industries and fields, such as public telecommunications and information services, power, transportation, water use, finance, public services, e-government, etc. and other key information infrastructures that, in the case of damage, lost function, or divulgence, may severely harm national security, the national economy or the public interest." Accordingly, under the

Cybersecurity Law, these data localization and export security assessment requirements only apply to enterprises that operate critical information infrastructure.

However, the Measures apply the data localization and export security assessment requirements to all network operators. Pursuant to Article 2 of the Measures, "personal information and important data generated or collected by a network operator during its operation within the territory of the People's Republic of China shall be stored within China. If it is necessary to transmit data abroad due to business needs, a security assessment shall be conducted in accordance with these Measures." In addition, Article 16 of the Measures requires that personal information and important data generated or collected by other persons and organizations within the territory of the People's Republic of China are to undertake security assessment work by referring to the Measures. While, theoretically, the provisions of this article do not have a direct mandatory effect on enterprises aside from network operators, persons and organizations that are referenced in the same or similar circumstances are clearly covered by new regulations in light of current legislative and regulatory trends in the cross-border transmission of personal information and important data.

From these two Measures provisions, it is clear that all enterprises engaging in cross-border data transmission are likely to be included in the scope of the security assessment, which will undoubtedly increase the cost and burden of corporate compliance, especially for enterprises in industries and activities involving cross-border enterprise management, financing activities, information services, data storage, technology research and development and network platforms, which will be subject to strict supervisory security assessments. We predict that this broadening of the applicable scope may receive a strong market response, and that some of the public comments will oppose this change.

Content to be supervised, regardless of data type

Articles 8, 9 and 11 of the Measures address assessment content, the need to report to the industry administrative or supervisory department and non-exportable data, respectively, to conduct the comprehensive supervision of different types and forms of cross-border data transmission.

a. Focus of Data Export Security Assessments

Article 8 of the Measures provides that data export security assessments shall focus on the following:

i. Necessity of transmitting the data abroad;

ii. Whether personal information is involved, including the quantity, scope, type, the sensitivity of the personal information, as well as whether the information subject consents to transmit the information abroad;

iii. Whether important data is involved, including the quantity, scope, type and sensitivity of the important data;

iv. The security protection measures, ability and standards of the data receiver, as well as the network security environment of the country or region where the data receiver is located;

v. The risk of divulgence, damage, alteration or misuse of the data transmitted abroad and further transferred;

vi. The potential risk to national security, social and public interests, and legitimate personal interests arising from transmitting the data abroad and gathering the data to be transmitted abroad;

vii. Other important matters required to be assessed.

With respect to the export of personal information, the Measures require that network operators explain to personal information subjects the purpose, scope, content and the receiver of the data to be transmitted abroad, as well as the country or region where the receiver is located, and it is necessary to receive the subject's consent. In the case of the personal information of minors, consent of a guardian is required. Besides these requirements, Article 12 of the Measures requires a re-assessment to be performed timely where the data receiver changes, or where a substantial change occurs to the purpose, scope, quantity, type or receiver of the data, or when a significant security incident has occurred with the exported data.

b. Reporting data export security assessments

Article 9 of the Measures provides that network operators shall report to the industry administrative or supervisory department to organize a security assessment where the data to be exported falls under one of the following circumstances:

i. It contains or in aggregate contains the personal information of more than 500,000 persons;

ii. The data exceeds 1,000 gigabytes;

iii. It contains data on nuclear facilities, chemical biology, national defense, population health, etc., large-scale project activities, marine environments and sensitive geographic data, etc.;

iv. Cybersecurity information that contains system vulnerabilities of key information infrastructures, security protections, etc.;

v. Operators of key information infrastructure that transmit personal information and important data abroad;

vi. Other circumstances that may potentially affect national security and the social public interest that the industry administrative or supervisory department determines should be assessed.

The Measures require that security assessments be completed within 60 working days, that network operators be given timely feedback and the results be reported to the CAC. The CAC

will organize the assessment in cases where the industry administrative or supervisory department is unclear.

c. Non-exportable Data

Article 11 of the Measures provides that certain data cannot be exported, including:

i. Where the personal information subject has not consented to the export of such information, or the export of data infringes on personal interests;

ii. Where the export of data poses risks to national politics, the economy, technology, national defense, etc., may affect national security, or harms the social and public interest;

iii. Other data as determined by the CAC, Public Security Bureau, security departments and other relevant departments.

The above provisions of the Measures carry out nearly complete supervision of cross-border data transmission, from the of focus and method of the assessment to the nature and quantity of the data, based on an expanded scope of persons subject to assessment.

Taking responsibility – enterprises will bear the burden

Articles 6, 7, 9 and 12 of the Measures provide for the specific methods for data export security assessments. Before data is to be exported, enterprises are to perform a self-assessment. Generally, enterprises that undertake data export security assessments themselves are responsible for the results of those assessments. Under special circumstances, including circumstances specified above, enterprises will report to the industry regulatory or supervisory department for a security assessment, and the department will decide whether the data can be exported.

We consider these provisions to deliver a clear signal emphasizing that enterprises are responsible for themselves: in general situations (Article 6), enterprises are to conduct and are responsible for self-assessments; in special circumstances (Article 9), enterprises must report to the relevant authorities for assessments. It is clear that enterprises are the primary actors and undertake liability with respect to data security assessments. Therefore, enterprises may be asked to make corrections or even be punished by their regulators if they fail to conduct assessments or engage in any concealed or fraudulent behavior in general, or fail to report to industry administrative or supervisory department for an assessment before transmitting data abroad under special circumstances.

How should enterprises approach these changes?

There is no doubt that the Measures will provide further guidance to enterprises in improving their data storage and cross-border transfer compliance by providing definitions and interpretations for some of the conceptual terms referenced in the Cybersecurity Law.

However, some Cybersecurity Law concepts waiting to be clarified remain unclear in the Measures, and the Measures themselves give rise to several pending issues.

For example, the concept of "important data" is defined as "data closely related to national security, economic development, and the social public interest…" However, what specifically constitutes important data is to be provided in a yet-unreleased reference guide. Furthermore, critical information infrastructure operators are required to request a security assessment when transmitting personal information and important data abroad. The State Council still has yet to formally introduce the relevant documents that provide what specifically constitutes "critical information infrastructure" beyond the definitions in the Cybersecurity Law and the widely referenced "State Cybersecurity Inspection Operation Guide," and the Measures provide no additional clarity in this respect. With the coming effectiveness of the Cybersecurity Law, these ambiguous concepts may lead to greater uncertainty and increased compliance risks for enterprises exporting data. In addition, since the Measures provide that "personal information without the consent of the information subject" cannot be exported, how is effective consent to be obtained from information subjects? This is of particular importance to banking, finance, healthcare, Internet and other public service industries that cover a broad range of information subjects.

Given this, while the Cybersecurity Law is being formally implemented and the supporting documents remain incomplete, we recommend that enterprises consider the following taking the following steps:

a. Establish sufficient internal control policies and data export security assessment mechanisms. For those enterprises that already have relevant policies or mechanisms, review those policies or mechanisms based on compliance with the Measures. Meanwhile, by referring to the key data export assessment criteria in Article 8 of the Measures, prepare the necessary analysis of data exports with respect to the type and amount of data to be exported from the perspectives of management, business, marketing, finances or other aspects of the company.

b. Develop and improve software and hardware for information protection and data security, understand the cybersecurity conditions in the countries or regions where information is to be sent, and make sure of effective links with offshore receivers of exported data.

c. Last and most importantly, enterprises should carry out effective communication with their industry administrative or supervisory department before transmitting data or information abroad, so as to first report the possible export of data and to understand whether the exported data is subject to self-assessment or reporting for assessment in order to significantly reduce compliance costs and risk when transmitting data.

● 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.

Should you have any questions regarding this publication, please contact **Mr. David TANG（+8621-6080 0905; david.tang@hankunlaw.com** ） or **Mr. Min ZHU** （ **+8621-6080 0955; min.zhu@hankunlaw.com**）.