Legal Commentary

March 23, 2024

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

BEIJING | SHANGHAI | SHENZHEN | HONG KONG | HAIKOU | WUHAN | SINGAPORE | NEW YORK

New Regulations on Cross-Border Data Flows Officially in Effect

Authors: Angus XIE | Huayi CHEN | Jiyan LIU

The Cyberspace Administration of China (CAC) issued the *Provisions on Regulating and Promoting Cross-Border Data Flows (Draft for Comments)* (《规范和促进数据跨境流动规定（征求意见稿）》) on September 28, 2023 seeking public comments, which garnered significant attention. Yesterday (March 22, 2024), the CAC issued the official version of the *Provisions on Promoting and Regulating Cross-Border Data Flows* (《规范和促进数据跨境流动规定》) (the "**Official Provisions**"), which came into effect immediately upon publication.

Meanwhile, the CAC also issued the *Guide to the Application for Security Assessment of Outbound Data Transfers (Second Edition)* (《数据出境安全评估申报指南（第二版）》) and the *Guide to the Filing of the Standard Contract for Outbound Transfer of Personal Information (Second Edition)* (《个人信息出境标准合同备案指南（第二版）》), providing detailed procedural guidance for data processors. Data processors can now use the "Outbound Data Transfers Application System" (https://sjcj.cac.gov.cn) to apply for security assessment of outbound data transfers and file standard contracts for outbound personal information transfers.

Main content of the Official Provisions

The Official Provisions clarify the applicable standards for data processors in cross-border data transfers, including security assessment, standard contract for outbound transfer of personal data, and personal information protection certification. The main contents of the provisions are as follows:

Security assessment of outbound data transfers: Critical information infrastructure operators (CIIOs) shall undergo a security assessment when transferring personal information or important data outside China. Other entities also need to conduct a security assessment when transferring important data or a large volume of personal information, with specific thresholds set at personal information (without sensitive personal information) of more than 1 million individuals or sensitive personal information of more than 10,000 individuals accumulated from January 1 of the current year.

Standard contract of outbound personal information transfers (or personal information protection certification): Non-CIIO entities transferring non-sensitive personal information of more than 100,000 but less than 1 million individuals must enter into a standard contract with the offshore recipient or obtain personal information protection certification. For the transfer of sensitive personal information, a standard contract or personal information protection certification must be obtained even if the volume is less than 10,000.

Firstly, the most significant difference between the Official Provisions and the draft provisions for public comments is the further clarification of the distinction between sensitive and non-sensitive personal information in outbound data transfer regulation, and the adjustment of the quantity thresholds for security assessment and personal information outbound transfer standard contracts (or personal information protection certifications) accordingly.

Specifically, for non-CIIO entities, the Official Provisions set the threshold for security assessment at personal information (without sensitive personal information) of more than 1 million individuals or sensitive personal information of more than 10,000 individuals per year. The threshold for personal information outbound transfer standard contracts (or personal information protection certifications) is set at non-sensitive personal information of more than 100,000 but less than 1 million individuals. For the outbound transfer of sensitive personal information, a standard contract or personal information protection certification is required even if the volume is less than 10,000.

In contrast, the draft provisions previously stipulated that the outbound transfer of personal information of less than 10,000 individuals to foreign entities within a year would not require the outbound data transfer security assessment, personal information outbound transfer standard contract, or personal information protection certification, without distinguishing between general and sensitive personal information.

Therefore, the Official Provisions reflect a further relaxation of regulation for general personal information, while increasing regulation for sensitive personal information. **As a result, companies transferring a small amount of sensitive personal information outside China could not be exempt from entering into a personal information outbound transfer standard contract under the Official Provisions as contemplated under the draft provisions.**

Secondly, the Official Provisions provide clearer requirements for the compliance obligations of CIIOs. The draft provisions previously stipulated that state organs and CIIOs transferring personal information and important data to offshore entities should follow relevant laws, administrative regulations, and departmental rules. In contrast, the Official Provisions clarify that CIIOs must undergo a security assessment when transferring personal information or important data outside China, with other data being exempted.

In addition, the Official Provisions continue the trend of relaxed regulation from the draft provisions in other aspects, as reflected in the following exemptions for applying for outbound data transfer security assessment, entering to personal information outbound transfer standard contract, and obtaining personal information protection certification:

1. **Important data**: Data processors should identify important data according to relevant regulations. For data that has not been notified or publicly released as important data by relevant departments or local government, data processors do not need to apply for security assessment on the basis of important data.

2. **Negative list of Free Trade Pilot Zones**: Free Trade Pilot Zones of China could set forth a negative list of data which should be subject to security assessment, standard contract or personal information protection certification under the data classification and graded protection system of the State. The negative list will become effective upon approval and registration. After that, outbound transfer of data by entities within the Free Trade Pilot Zones would be exempt from security assessment, standard contract or personal information protection certification if the data does not fall within the negative list.

3. **Data category exemption**: The provision of data collected and generated in international trade, cross-border transportation, academic cooperation, transnational manufacturing, and marketing activities overseas with no personal information or important data is exempt from outbound data transfer security assessment, personal information outbound transfer standard contract and personal information protection certification.

4. **Overseas data exemption**: The offshore provision of personal information collected and generated overseas by the data processors and transmitted to China for processing is exempt from outbound data transfer security assessment, personal information outbound transfer standard contract and personal information protection certification, provided that no domestic personal information or important data is introduced during the processing.

5. **Specific scenario exemptions**:

- Where personal information has to be transferred outside China for the purpose of entering into or performing contracts to which the individual is a contracting party, such as in the event of cross-border shopping, cross-border remittance, cross-border account opening, air ticket and hotel booking, visa application processing and examination services, etc.;
- Where employees' personal information has to be transferred outside China for the purpose of implementing human resource management under the employment policies established and collective employment contracts signed in accordance with the law; and
- Where personal information has to be transferred outside China in order to protect the life, health and property safety of natural persons in case of emergency.

6. **Volume-based exemption**: Non-CIIO entities who provides personal information records (without sensitive personal information) of less than 100,000 individuals outside China since January 1st of the current year.

Identification of sensitive personal information, important data, and CIIOs

Due to the above changes, the identification of concepts such as sensitive personal information, important

data, and CIIOs is crucial for understanding the specific scope of application of the Official Provisions. The CAC also responded specifically to these issues in its answers to journalists' questions.

Sensitive personal information

Sensitive personal information refers to personal information that, if disclosed or misused, could easily lead to the infringement of an individual's personal dignity or endanger personal and property safety. This includes biometric information, religious beliefs, specific identities, medical health, financial accounts, whereabouts and other information, as well as the personal information of minors under the age of 14.

The Information Security Technology — Personal Information Security Specification (《信息安全技术 个人信息安全规范》) (GB/T 35273-2020) provides more specific guidance on the identification of sensitive personal information, with the following examples of sensitive personal information according to the specification:

Category	Example information
Personal property information	Bank accounts, authentication information (passwords), deposit information (including fund amounts, payment and receipt records, etc.), property information, credit records, credit reporting information, transaction and consumption records, account activity, etc., as well as virtual currencies, virtual transactions, game redemption codes, and other virtual property information.
Personal health and physiological information	Records related to personal illness and treatment, such as symptoms, hospitalization logs, physician's orders, test results, surgical and anesthesia records, nursing notes, medication history, drug and food allergy information, reproductive health information, past medical history, diagnosis and treatment situation, family medical history, current medical history, infectious disease history, etc.
Personal biometrical information	Personal genes, fingerprints, voiceprints, palm prints, earlobe geometry, iris patterns, facial recognition features, etc.
Personal identity information	Identity cards, military officer certificates, passports, driver's licenses, work permits, social security cards, residence permits, etc.
Other information	Sexual orientation, marital history, religious beliefs, undisclosed criminal records, communication records and content, contact lists, friend lists, group memberships, travel histories, web browsing history, accommodation information, precise location data, etc.

Important data

According to the *Measures for Security Assessment of Outbound Data Transfers*, important data refers to data that, if tampered with, destroyed, disclosed, or illegally obtained or utilized, may endanger national security, economic operations, social stability, public health and safety, etc.

The *Data Security Law* stipulates that the national data security work coordination mechanism shall coordinate with relevant departments to develop the important data catalogs and strengthen the protection of important data. Local governments and departments should determine the specific catalog of important data for their region, department, and relevant industry or field according to the data classification and graded protection system, and protect the data included in the catalog as a priority.

For the identification of important data, further clarification will be provided in documents such as the draft for approval of the *Data Security Technology — Data Classification and Grading Rules* (《数据安全技术 数据分类分级规则》) (GB/T 43697-2024) and the daft for comments of the *Information Security Technology — Important Data Identification Guide* (《信息安全技术 重要数据识别指南》).

In this regard, the Official Provisions clarifies that if data has not been notified or publicly released as important by relevant departments or local governments, data processors do not need to apply for security assessment on the basis of important data, providing companies with greater certainty.

Critical information infrastructure operators

According to the *Regulations on the Security Protection of Critical Information Infrastructure* (《关键信息基础设施安全保护条例》), critical information infrastructure refers to important network facilities and information systems in public communication and information services, energy, transportation, water conservancy, finance, public services, electronic government affairs, defense science and technology industry, and other important industries and fields, as well as others that, if damaged, lose function, or have data leaked, may seriously endanger national security, national economy and people's livelihood, and public interest.

The competent departments and supervisory bodies responsible for the important industries and fields involved shall formulate the rules for identifying critical information infrastructure in their industry or field, organize the identification of critical information infrastructure in their industry or field, and promptly notify the CIIOs of the identification results.

In practice, similar to important data, if a company has not been explicitly notified by the relevant departments, it does not need to assume that it is a CIIO.

Impact on companies and recommendations

Facing the Official Provisions, companies should take the following measures to ensure compliance:

Personal information outbound transfer scenario evaluation: Companies should re-evaluate their data transfer activities, grasp the data scenarios in their business operations and daily management, and the specific categories and quantities of data transferred, and determine the data outbound transfer compliance obligations they should fulfill corresponding to the Official Provisions;

Identification of sensitive personal information: Since the Official Provisions require that for the outbound transfer of sensitive personal information, even if the volume is less than 10,000, a standard contract or personal information protection certification must be fulfilled, companies should pay special attention to whether there is any sensitive personal information in their data transferred that does not

belong to the exempted scenarios. For example, the ID numbers and bank account information of employees transferred abroad by the company can be exempted, while the ID numbers of contact persons from other cooperating parties may not be exempted and require entering into a standard contract;

Continuous obligations: Even in the exempted scenarios of security assessment, standard contract and personal information protection certification, companies still have obligations regarding the outbound transfer of personal information, including the obligation to inform, obtain individual separate consent, conduct personal information protection impact assessments. For any outbound data, they must also fulfill data security protection obligations, take technical and other necessary measures to ensure the security of data transfers, and in the event of a data security incident or a possible occurrence, take remedial measures and report promptly to the provincial-level or higher cyberspace administration departments and other relevant competent departments.

In summary, the new regulations provide clearer guidance and requirements for cross-border data flows, and companies need to closely monitor these changes and promptly adjust their data management and protection strategies to ensure compliance and protect the rights and interests of both the companies and their users.

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:

Angus XIE

Tel: +86 10 8524 5866
Email: angus.xie@hankunlaw.com