环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

威科 Wolters Kluwer

NIO蔚来

奇安信

Ogilvy

YOUZAN

Outbound Cross-Border Data Transfer Compliance Guideline

50 Common Questions

2025 Edition

PREAMBLE

With the booming development of the digital economy, data has become an important factor of production and a key driver of development. Cross-border data flow is essential as a strategic leverage for global economic development, technological innovation and international trade. However, cross-border data flow presents challenges and controversies in terms of data security and privacy protection. Many countries have therefore intensified the regulation and standardization of cross-border data flow.

On July 7, 2022, Cyberspace Administration of China (CAC) released ***the Measures for the Security Assessment of Cross-Border Data Transfer*** (effective on September 1, 2022). With other previously released laws and regulations, it established an initial regulatory framework for outbound cross-border data transfer compliance. However, ambiguities in the rules and regulations resulted in initial uncertainty for many enterprises. On September 28, 2023, CAC released ***the Regulations on Regulating and Promoting Cross-Border Data Flow (Draft).*** It sparked extensive discussions in various sectors regarding the selection of appropriate outbound cross-border data transfer compliance measures.

On March 22, 2024, after six months of reviewing and considering external feedback, CAC officially announced ***the Regulations on Promoting and Regulating Cross-Border Data Flow*** (***the Regulations on Cross-Border Data Flow***) which became effective immediately. ***The Regulations on Cross-Border Data Flow*** refined the regulatory framework for outbound data transfer, further easing the requirements for data transfer and narrowing the scope of security assessment for cross-border data transfer. These latest regulatory update showed CAC's intention to facilitate and promote cross-border data flow, by reducing the cost of compliance and promoting the growth of trade and the digital economy, while balancing data security and national interests.

As ***the Regulations on Cross-Border Data Flow*** will impact enterprises' who may need to transfer data outside the Chinese mainland, the data and cyber security team

from Global Law Office, in conjunction with University of International Business and Economics Research Center for Digital Economy and Legal Innovation, NIO Holdings Ltd., Qi An Xin Technology Group Inc., Beijing Ogilvyone Marketing Co.Ltd., and Hangzhou Youzan Technology Co., Ltd., have collaborated to release this guideline to help answer common questions on cross-border data transfer in a FAQ format. This guideline, is divided into two parts: the first part introduces the legal and regulatory framework of cross-border data transfer in the Chinese mainland, addresses the relevant concepts, and proposes precautions. The second part analyzes common cross-border data transfer scenarios, data types and the process of outbound cross-border data transfer security assessments and submission, as well as risk assessments and counter measures.

In the era of rapid growth in digital economy, compliance management of cross-border data transfer will become an essential capability for enterprises. We hope that the release of this article**.** will provide a useful reference for enterprises who need to move and share data between countries and regions.

Finally, we would like to thank all the participating organizations and personnel for the hard work, especially the strong support of Wolters Kluwer, and everyone for their valuable input and advice.

Meng, Maggie (Jie)

CONTENTS

PREAMBLE **1**

PART 1 FUNDAMENTALS **1**

I. What are the Legal and Regulatory Requirements Governing Cross-Border Data Transfer in China? 2

II. What Activities Constitute Cross-Border Data Transfer? 11

III. How to Identify Overseas Recipient of Outbound Cross-Border Data Transfer? . 12

IV. What are the Three Routes for China's Current Outbound Cross-Border Data Transfer System? How Can One Determine Which Route to Select? 13

V. Under What Scenarios can Data be Transferred outside the Chinese mainland without Following the Three Routes of Outbound Cross-Border Data Transfer? 17

VI. Which Scenarios Fall under the Category of "Laws and Administrative Regulations Provide Otherwise, and Assessment/Approval Shall be Submitted in Accordance with Their Provisions"? 23

VII. Which Scenarios Fall under the Category of "Laws and Administrative Regulations Provide Otherwise, and Assessment/Approval Shall be Submitted in Accordance with Their Provisions"? 24

VIII. What is the Procedure of Outbound Cross-Border Data Transfer Security Assessment? 25

IX. How long will Outbound Data Transfer Security Assessment Submission Take? 29

X. Under What Scenarios Can an Enterprise Choose to Conclude and File the Standard Contract for the Outbound Transfer of Personal Information? 30

XI. What is the Process of Concluding and Filing the Standard Contract for the Outbound Cross-Border Transfer of Personal Information? 31

XII. Under What Scenarios Can an Enterprise Choose to Obtain the Personal Information Protection Certification? 35

XIII. What is the Process of Obtaining a Personal Information Protection Certification? 36

XIV. What are the CIIO Outbound Data Transfer Requirements? 44

XV. What are the Legal and Regulatory Bases for Identifying Important Data?

.....45

XVI. What are the Requirements for Outbound Transfer of Important Data? 47

XVII. What are the Specific Contents of the Standard Contract for the Outbound Transfer of Personal Information? 48

XVIII. What are the Specific Requirements for the Personal Information Protection Certification?.....49

XIX. What are the Penalties for Failing to Comply with the Outbound Data Transfer Regulations?.....54

XX. What other Specific Matters should be Noted?.....55

XXI. Does China's Guangdong-Hong Kong-Macao Greater Bay Area Have Special Facilitation Measures for Outbound Cross-Border Transfer of Personal Information? 56

PART 2 PRACTICE 59

XXII. How to Identify Scenarios of Cross-Border Data Transfer? 60

XXIII. What are Potential Cross-Border Data Transfer Scenarios that Enterprises May be Involved in?.....66

XXIV. How to Accurately Identify the Type of Cross-Border Data Transfer?.....70

XXV. How to Account for the Quantity of Data Transferred Across Border？ 71

XXVI. How to Identify Internal Department Responsible for the Implementation of Compliance Measures for Cross-Border Data Transfer? 74

XXVII. How to Determine the Submission of the Outbound Cross-Border Data Transfer Security Assessment? 75

XXVIII. How to Determine the Timing for Outbound Cross-Border Data Transfer Security Assessment?.....77

XXIX. Which Organization(s) Should the Enterprise Submit Outbound Cross-Border Data Transfer Security Assessment?.....78

XXX. How to Submit a Personal Information Protection Impact Assessment?.....79

XXXI. How to Submit Outbound Cross-Border Data Transfer Risk Self-Assessment? 81

XXXII. Are PIAs and the Self-Assessment of Cross-Border Transfer Risks the Same in the Scenario of Cross-Border Data Tansfer?.....85

XXXIII. How to Assess Whether the Technical and Organizational Measures of Data

Processors and Overseas Recipient are Adequate? 88

XXXIV. How to Assess the Adequacy of the Overseas Recipient's Legal and Policy Environment? 91

XXXV. What is the European Union's Approach to Assess Data Security Protection Policies and Legislation, as well as the Cybersecurity Environment? 95

XXXVI. For How Long will a Outbound Cross-Border Data Transfer Security Assessment Result Remain Valid? Under What Scenarios is it Necessary to Resubmit for a Security Assessment? 98

XXXVII. Under What Scenarios is it Necessary to Re-Conclude the Standard Contract and Record Submission for Cross-Border Transfer of Personal Information? 99

XXXVIII. Is it Possible to Modify the Standard Contract issued by the Regulatory Authority? 100

XXXIX. If a Data Processing Agreement with an Overseas Recipient already Exists, is it Permissible to Include a Standard Contract as an Attachment? 101

XL. To whom should the Application of Personal Information Protection Certification be Submitted? 101

XLI. How should Cross-Border Data Transfer be Properly Managed in the Context of International Dispute Resolution? 104

XLII. How to Sign and Record the Submission of China's GBA Standard Contract for Cross-Border Transfer of Personal Information? 107

XLIII. Are There any Regulatory Measures to Facilitate the Outbound Personal Information Transfer in the Shanghai Pilot Free Trade Zone? 109

XLIV. Are There any Special Regulations for the Data Transfer in the Banking and Finance Industry? 112

XLV. Are There any Special Regulations for the Outbound Transfer of Data in Securities and Fund Industry? 115

XLVI. What are the Common Scenarios of Cross-Border Data Transfer in the Pharmaceutical Industry? 118

XLVII. What are the Types of Data Involved in Cross-Border Data Transfer in the Pharmaceutical Industry? 119

XLVIII. What are the Major Compliance Obligations for the Cross-Border Data Transfer for the Pharmaceutical Industry? 121

XLIX. What Cross-Border Data Compliance Issues Should be Considered for Cross-Border Data Trade through Domestic Data Exchanges? 124

L. Can Public Data Operators Authorize or Share Public Data with Overseas Entities? 127

Annex I. The National and Provincial Cyberspace Administration Contact Information 130

Annex II. Glossary Reference 134

PART 1 FUNDAMENTALS

I. What are the Legal and Regulatory Requirements Governing Cross-Border Data Transfer in China?

China's legislation on cross-border data transfer started relatively late. The restrictions and regulatory provisions for cross-border data transfer are dispersed across various laws, regulations, departmental rules, and normative documents. These provisions are continually being innovated and improved, gradually moving towards the establishment of a comprehensive and mature system .

The legal framework for outbound data transfer originates from ***the Cybersecurity Law of the People's Republic of China*** (***the Cybersecurity Law***), effective June 1, 2017. ***The Cybersecurity Law*** first mandated a security assessment requirement for outbound data transfer, requiring critical information infrastructure operators (**CIIO**) to submit a security assessment in accordance with the rules developed by the Cyberspace Administration of China (CAC) and relevant State Council departments when the CIIO provides personal information and important data overseas for business purposes[1]. On August 30, 2017, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (**TC260**) issued ***the Information Security Technology- Guidelines for Cross-Border Data Transfer Security Assessment (Draft for Comment)***(***the Guidelines for Security Assessment (Draft)***) , which provided guidance on the security assessment process, key assessment points, and assessment methods prior to the release of ***the Measures for the Security Assessment of Cross-Border Data Transfer***.

The Data Security Law of the People's Republic of China (***the Data Security Law***), effective on September 1, 2021, reiterated the requirement for CIIOs to assess important data collected and generated domestically before conducting cross-border data transfer. It also established principles for regulating the outbound transfer of important data by other data processors[2]. Additionally, ***the Data Security Law*** imposed restrictions on transferring data to foreign judicial and law enforcement agencies, requiring the domestic entities and individuals to obtain approvals from relevant authorities before providing data stored within the Chinese mainland to foreign agencies[3]. Subsequently, ***the Personal Information Protection Law of the People's***

[1] See Article 37 of *the Cybersecurity Law*.
[2] See Article 31 of *the Data Security Law*.
[3] See Article 36 of *the Data Security Law*.

Republic of China (***the Personal Information Protection Law***) that was implemented on November 1, 2021, similarly stipulates that "without the approval of the competent authorities personal information processors may not provide personal information stored within the Chinese mainland to foreign judicial or law enforcement agencies".

The Personal Information Protection Law was quickly followed by ***the Regulations on Network Data Security Management (Draft for Comment)*** (***the Network Security Management Regulations (Draft)***), which specifically focuses on regulating Cross-Border Data Security Management[4]. Article 38 of ***the Personal Information Protection Law*** and Article 35 of ***the Network Security Management Regulations (Draft)*** outline three main compliance routesroutes for cross-border transfer[5]:

1. Completing and obtaining approval for a data security assessment as required by the cyberspace authority,

2. Obtaining personal information protection certification from professional institutions in accordance with the regulations of the cyberspace authority,

3. Concluding contracts with overseas recipients in accordance with the standard contracts stipulated by the cyberspace authority, specifying the rights and obligations of both parties

These procedures collectively are referred to as *the Outbound Data Transfer Procedures*.

Subsequently, to promote the implementation of the above outbound data transfer systems, the CAC and the relevant regulatory authorities of different industries have issued further rules, guidance and policies and are expected to continue to do so. Regarding Personal Information Protection Certification, the relevant industrial regulatory authority and the CAC jointly issued ***the Announcement on the Implementation of Personal Information Protection Certification*** (***the Certification Announcement***) and ***the Certification for Personal Information Protection Implementation Rules*** (***the Certification Rules***) on November 4, 2022. These documents set out the basic rules for carrying out personal information protection

[4] See Chapter 5 of *the Network Security Management Regulations (Draft)*.
[5] See Article 38 of *the Personal Information Protection Law*.

certification, marking the official establishment of the personal information protection certification system in China. In June 2022, the Information Security Standards Committee released ***the Guidelines to Cybersecurity Standards - Specification on Security Authentication for Cross-Border Personal Information processing Activities*** (***the Certification Specification V1.0***) , further providing support for the personal information protection certification rules.

In December 2022, **TC260** released ***the Guidelines to Cybersecurity Standards - Specification on Security Authentication for Cross-Border Personal Information processing Activities V2.0*** (***the Certification Specification V2.0***), which elaborated on ***the Certification Specification V1.0*** in five aspects: the content that legally binding agreements should cover, the responsibilities of personal information protection institutions, the issues that personal information impact assessments should cover, the rights of personal information subjects, and the responsibilities and obligations of personal information processors and overseas recipients. On March 16, 2023, **TC260** issued the national standard ***Information Security Technology - Certification Requirements for Cross-Border Transfer of Personal Information (Draft for Comment)*** (***the Certification Requirements for Cross-Border Transfer (Draft)***), a recommended national standard with greater legal weight than ***the Certification Specification V2.0***. Apart from introducing the definitions of s*ensitive personal information* and *separate consent* and removing the related requirements for the certification applicant, the overall content of ***the Certification Requirements for Cross-Border Transfer (Draft)*** remains consistent with ***the Certification Specification V2.0***. On November 1, 2023, following ***the Memorandum of Cooperation on Promoting Cross-Border Data Flow in the Guangdong-Hong Kong-Macao Greater Bay Area*** and relevant local laws and regulations, **TC260** established ***the Guidelines to Cybersecurity Standards - Requirements for Protection of Cross-border Personal Information in Guangdong-Hong Kong-Macao Greater Bay Area (Draft for Comment)***, specifying the basic principles and protection requirements for cross-border processing of personal information in the Greater Bay Area and setting a foundation for the implementation of the personal information protection certification in that area.On January 3, 2025, the CAC released ***the Measures for the Certification of Personal Information Protection for Outbound Personal Information Transfer(Draft for Comment)*** （*the Certification Measures for Outbound Personal Information Transfer*

(Draft)》, which provides a clear legal basis and a feasible compliance operation scheme for the cross-border personal information transfer, by establishing the certification of personal information protection as one of the compliance paths for outbound data transfer.

Regarding the Outbound Cross Border Data Transfer Security Assessment, the CAC issued ***the Measures for the Security Assessment of Cross-Border Data Transfer*** (***the Assessment Measures***) on July 7, 2022, which took effect from September 1, 2022. The measures specify the particular scenarios and requirements for security assessment for an outbound cross-border data transfer. For the Standard Contract for the Outbound Transfer of Personal Information, the CAC released on February 22, 2023 ***the Measures for the Standard Contract for Cross-Border Transfer of Personal Information*** (***the Measures for the Standard Contract***) which took effect from June 1, 2023. These measures specify the scenarios where enterprises can choose to execute and file standard contracts with overseas recipients.

In order to optimize the outbound data transfer systems, while considering the need to ensure a refined alignment with the security risks, a targeted and differentiated approach is promoted for security measures.

In order to promote and regulate the lawful and orderly free flow of data and based on practical experience in managing outbound data security, the CAC released a significant document on March 22, 2024, ***the Regulations on Promoting and Regulating Cross-Border Data Flow*** (***the Regulations on Cross-Border Data Flow***).

The Regulations on Cross-Border Data Flow optimizes systems for outbound data transfer in five key ways:

1. Clarifying the criteria for identifying important data.

2. Proposed scenarios for outbound data transfer activities that are exempted from submitting the Outbound Cross-Border Data Transfer Security Assessment, concluding the Standard Contract for the Outbound Transfer of Personal Information, and obtaining the Personal Information Protection Certification.

3. Establishing a negative list for free trade pilot zones.

4. Adjusting the threshold standards by easing the scenarios for cross-border data

flow and narrowing down the scope for the Outbound Cross-Border Data Transfer Security Assessment.

5. Extending the validity period of the Outbound Cross-Border Data Transfer Security Assessment.

Additionally, to accompany the implementation of ***the Regulations on Cross-Border Data Flow***, the CAC released on the same day ***the Guidelines to Submission for Security Assessment of Outbound Data Transfers (Second Edition) (the Guidelines to Assessment Submission (Second Edition))*** and ***the Guidelines to Recording Submission of Standard Contract for Outbound Cross-border Transfer of Personal Information (Second Edition)*** (***the Guidelines to Recording Submission of Standard Contract (Second Edition)***). These guidelines provide detailed requirements for the methods, processes, and materials needed for submitting outbound cross-border data transfer security assessment and filing standard contracts for the outbound transfer of personal information. They also optimize and simplify the materials that data processors need to submit.

The introduction of ***the Regulations on Cross-Border Data Flow***, ***the Guidelines to Assessment Submission (Second Edition)*** , and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)*** reflects the regulatory authorities' evolving approach on outbound data transfer governance. This approach aims to ensure the lawful and orderly flow of data, providing legal protection for organizations and individuals engaging in cross-border business cooperation, while also promoting the free movement of data. It further advances the development of the free flow of data and the digital economy.

On one hand, the new regulations clarifies that regulatory bodies will strengthen comprehensive oversight before, during, and after data processing. This includes enhancing guidance and supervision of data processors who provide data outside the Chinese mainland, ensuring they fulfill obligations such as notification, obtaining individual consent, submitting Personal Information Protection Impact Assessment, implementing technical measures to ensure data security during outbound cross-border transfer, and reporting outbound data security incidents to provincial-level cyberspace authorities and other relevant regulatory bodies.

On the other hand, by streamlining the mechanism for cross-border data transfer

systems, a new framework for digital cross-border trade has been established, encouraging the businesses to actively engage in cross-border data flow and promote international trade development. For different business activity scenarios, where no personal information or important data is involved, the regulations allow outbound data in the international trade, cross-border transport, academic cooperation, transnational production, and marketing to be exempted from submitting the Outbound Cross-Border Data Transfer Security Assessment, concluding the Standard Contract for the Outbound Transfer of Personal Information, and obtaining the Personal Information Protection Certification. This releases compliance costs for many businesses.

The release of ***the Regulations on Cross-Border Data Flow*** marks a new phase for enterprise compliance activities in the cross-border data transfer. These regulations not only improve the practicality and operability of the current outbound data transfer systems but also actively address the common concerns of the enterprises regarding compliance in cross-border data transfer, thereby reducing the compliance challenges and complexities businesses face in outbound data transfer activities. In light of this, businesses involved in cross-border data transfer can deploy this opportunity to systematically review their outbound data transfer scenarios and the corresponding compliance procedures under the rules. By doing so, they can ensure compliance with the regulatory boundaries while actively pursuing international operations and cross-border business cooperation.

Nearly three years after the CAC released ***the Regulations on Network Data Security Management (Draft)***, the 40th Executive Meeting of the State Council adopted ***the Regulations on Network Data Security Management*** (***the Network Security Management Regulations***) on August 30, 2024. ***The Network Security Management Regulations*** were officially promulgated on September 24, 2024, and will come into effect on January 1, 2025. Chapter 5 of ***the Network Security Management Regulations*** outlines security management requirements for cross-border data transfer, with a focus on the following aspects:

1. Compliance Requirements for Providing Personal Information Outside the Chinese mainland

Building on the experience gained from the formulation and implementation of departmental regulations such as ***the Assessment Measures for Data Transfer***, ***the***

Measures for the Standard Contract and ***the Regulations on Cross-border Data Flow***, ***the Network Security Management Regulations*** further clarify the role and functions of the national cybersecurity authorities in cross-border data activities while optimizing China's outbound data transfer system. Article 35 of ***the Network Security Management Regulations*** stipulates seven conditions for providing personal information to overseas entities, along with a catch-up clause. These conditions integrate the three main compliance routes and include the exemption scenarios provided in ***the Regulations on Cross-border Data Flow***. Additionally, Article 36 of ***the Network Security Management Regulations*** addresses special scenarios for providing personal information outside the Chinese mainland based on international treaties and agreements China has joined. As a result, there are now eight conditions under which personal information can be lawfully transferred outside the Chinese mainland:

1)Passing the Outbound Cross-Border Data Transfer Security Assessment: Completion of the Outbound Cross-Border Data Transfer Security Assessment organized by the national cybersecurity authority.

2) Obtaining the Personal Information Protection Certification: Certification of personal information protection conducted by a professional organization in accordance with regulations set by the national cybersecurity authority.

3) Concluding the Standard Contract for the Outbound Transfer of Personal Information: conclusion of a standard contract, formulated by the national cybersecurity authority, with the overseas recipient, stipulating the rights and obligations of both parties.

4) Contract Fulfillment: Personal information must be provided outside the Chinese mainland for the establishment or performance of a contract in which the individual is a party.

5) Human Resources Management: cross-border human resources management that requires providing employees' personal information outside the Chinese mainland, implemented in accordance with legally formulated labor regulations and collective agreements.

6) Fulfilling Legal Obligations: Provision of personal information outside the

Chinese mainland is required to fulfill statutory duties or obligations.

7) Emergency Scenarios: In emergency scenarios, personal information must be provided outside the Chinese mainland to protect the life, health, and property safety of natural persons.

8) Other Conditions Specified by Laws, Administrative Regulations, or the National Cybersecurity Authority: Provision of personal information outside the Chinese mainland under other specified conditions.

9) Provisions in International Treaties: If international treaties or agreements that the People's Republic of China has concluded or joined include conditions for providing personal information outside the Chinese mainland, those provisions may be followed.

2. Compliance Requirements for Providing Important Data Outside the Chinese mainland

Article 37 of ***the Network Security Management Regulations***, based on the provisions of ***the Assessment Measures for Data Transfer***, requires that network data processors intending to provide important data collected and generated during operations within the Chinese mainland to overseas entities must undergo a Outbound Cross-Border Data Transfer Security Assessment organized by the national cybersecurity authority.

Regarding the criteria for identifying important data, ***the Network Security Management Regulations*** reiterate two key points: 1) Necessity of Cross-Border Provision: Providing important data collected and generated during operations within the Chinese mainland to overseas entities must be strictly necessary. Enterprises are required to submit self-assessments, provide justification, and submit supporting materials to substantiate the necessity of the cross-border transfer.

2) Standards for Identifying Important Data: According to ***the Regulations on Cross-border Data Flow***, the determination of important data relies on notifications or public releases by local and industry regulatory departments. If an enterprise has not been notified by relevant departments or regions about processing important data, or if the data processed by the enterprise is not included in the publicly released directory of important data, the enterprise is not required to submit the data as important data for a

security assessment[6].

3. Other Compliance Obligations When Providing Data Outside the Chinese mainland

Building on the requirements outlined in ***the Assessment Measures for Data Transfer*** regarding the content of Outbound Cross-Border Data Transfer Security Assessment, Article 38 of ***the Network Security Management Regulations*** explicitly states that network data processors who provide personal information and important data outside the Chinese mainland after passing a data outbound security assessment must not exceed the purposes, methods, scope, categories, or scale of data transfer specified during the assessment. Therefore, enterprises must strictly adhere to the materials submitted during the assessment and the terms of the contract with the overseas recipient when conducting cross-border data transfer activities. If actual cross-border transfer activities exceed the scope of what was submitted during the assessment, the national cybersecurity authority may determine that the outbound data transfer activities no longer comply with the security management requirements for cross-border data transfer. Consequently, the national cybersecurity authority may, based on ***the Assessment Measures for Data Transfer***, require the enterprise to terminate its cross-border data transfer activities. If the enterprise wishes to continue such activities, it must make the necessary rectifications and reapply for assessment.

Furthermore, Article 39 of ***the Network Security Management Regulations*** emphasizes the responsibility of network data processors to prevent security risks during cross-border data transfer. From an implementation perspective, this includes measures taken by the state to prevent and address cross-border data security risks and threats. It also prohibits any individual or organization from providing programs, tools, or other means specifically designed to disrupt or bypass technical safeguards, aiming

---

[6] Currently, various regions in China are actively exploring the establishment of data classification and grading protection systems, as well as developing positive and negative lists for cross-border data flow to clarify the types of "important data". For example:
On February 5, 2024, the Tianjin Free Trade Zone took the lead in releasing the Standards and Specifications for Data Classification and Grading of Enterprises in the China (Tianjin) Pilot Free Trade Zone. This document categorizes data into 13 major types and 40 subtypes, with three levels: core, important, and general.
On February 8, 2024, the Shanghai Lingang New Area issued the China (Shanghai) Pilot Free Trade Zone Lingang New Area Cross-Border Data Flow Classification and Grading Management Measures (Trial). It proposed a classification and grading management system for cross-border data flow, along with mechanisms for the formulation, application, and updating of important data directories.
On August 26, 2024, the Beijing Free Trade Zone, in collaboration with the Beijing Cyberspace Administration and two other departments, published the China (Beijing) Pilot Free Trade Zone Cross-Border Data Negative List Management Measures (Trial) and the China (Beijing) Pilot Free Trade Zone Cross-Border Data Management List (Negative List) (2024 Edition). This initiative initially focuses on five sectors—automotive, pharmaceuticals, retail, civil aviation, and artificial intelligence. It provides detailed lists of important data in these fields, covering 18 data subtypes along with their key characteristics and descriptions, which require Outbound Cross-Border Data Transfer Security Assessment.

to curb the spread of hacking tools and similar resources in society. Additionally, knowingly providing technical support or assistance to individuals engaging in such disruptive activities is also prohibited. ***The Network Security Management Regulations*** makes it clear that even if individuals or organizations do not directly participate in the disruption or circumvention of technical safeguards, they can still bear legal responsibility for such acts. This measure is designed to effectively reduce *accomplice* behavior and further deter criminal activity.

II. What Activities Constitute Cross-Border Data Transfer?

The first part, the Submission Scope, of ***the Guidelines to Assessment Submission (Second Edition)*** and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)*** clearly define what constitutes Cross-Border Data Transfer. It includes three following scenarios:

- Transferring personal information or important data collected and generated within the Chinese mainland to overseas parties
- Storing such data outside the Chinese mainland while ensuring that it remains accessible to individuals or organizations within the Chinese mainland.
- Other activities that meet the scenarios outlined in the second paragraph of Article 3 of ***the Personal Information Protection Law***, which covers activities involving the processing personal information of natural persons within the Chinese mainland by entities outside the Chinese mainland. These activities include:①Processing personal information for the purpose of providing products or services to natural persons within the Chinese mainland ②Analyzing or evaluating the behavior of natural persons within the Chinese mainland.③Other scenarios as stipulated by laws and administrative regulations. Additionally, it includes other data processingactivities of natural persons within the Chinese mainland that are processed outside the Chinese mainland.

(For detailed content, please refer to "Part 2 Practice: XXII. How to Identify Scenarios of Cross-Border Data Transfer? ")

III. How to Identify Overseas Recipient of Outbound Cross-Border Data Transfer?

According to ***the Guidelines to Assessment Submission (Second Edition)***, even if data is not transferred outside the Chinese mainland, as long as the data is accessed, reviewed, or retrived by foreign institutions, organizations, or individuals (excluding public information and webpage access), such activities are identified as outbound data transfer. Similarly, if a domestic enterprise engages foreign service providers to directly collect personal information generated within the Chinese mainland through foreign servers, such activities are also identified as outbound cross-border data transfer.

The *overseas recipient* generally refers to the first-hand overseas data recipient. If multiple first-hand overseas data recipients are involved, data processors need to evaluate each recipient's ability in the self-assessment report to ensure the security of the outbound data transfer. Factors to be considered in the self-evaluation include, but are not limited to, business scenarios, the scale of outbound cross-border data, the purpose and method of data processing, and the management and technical measures implemented by the overseas recipient. Additionally, if the data will be transmitted to other overseas recipients after being transferred, this subsequent transmission must also be evaluated.

Generally, the relationship between multinational corporations (MNCs) and their third-party suppliers is entrusted data processing. Typically, the headquarters of the MNC directly engages the overseas suppliers and enters into a *Data Processing Agreement (DPA)*, stipulating that the MNC and its subsidiaries are the data controllers, and the supplier is the processor. In this context, if the overseas parent enterprise can access and review its Chinese subsidiary's data stored on overseas servers, and the *Data Processing Agreement* allows the overseas parent enterprise to process the data collected by the overseas supplier for its own purposes, then the overseas parent enterprise is the overseas recipient. Therefore, the Chinese subsidiary is transferring personal information to its overseas parent enterprise.

IV. What are the Three Routes for China's Current Outbound Cross-Border Data Transfer System? How Can One Determine Which Route to Select?

Based on the basic legal requirements of ***the Cybersecurity Law***, ***the Data Security Law***, and ***the Personal Information Protection Law***, when enterprises engage in outbound data transfer activities, they should consider the entity type and the data type and data amount being transferred to comprehensively to determine whether they need to (1) Submitting and Passing the Outbound Cross-Border Data Transfer Security Assessment; (2) Filing and Concluding the Standard Contract for the Outbound Transfer of Personal Information; or (3)Obtaining the Personal Information Protection Certification.

Specific details are shown in the table below.

Laws	Effective Date	Regulated Subject	Compliance Route
The Cyber Security Law	June 1st, 2017	CIIO	If CIIO needs to provide personal information and important data outside the Chinese mainland, they must submit a security assessment in accordance with the measures formulated by national cyberspace administration authority in collaboration with relevant departments of the State Council.
The Data Security Law	September 1st, 2021	CIIO	A security assessment is required if providing important data overseas.
		Data processors other than CIIO	When important data are transferred to overseas recipient, data processors must comply with the measures formulated by national cyberspace administration authority in collaboration relevant departments of the State Council.

<table>
<tr><th>Laws</th><th>Effective Date</th><th colspan="2">Regulated Subject</th><th>Compliance Route</th></tr>
<tr><td rowspan="3">The Personal Information Protection Law</td><td rowspan="3">November 1st, 2021</td><td colspan="2">CIIO</td><td>A security assessment is required if providing personal information overseas.</td></tr>
<tr><td rowspan="2">Data processors other than CIIO</td><td>Personal information processors who meet quantity requirement specified by the national cybersecurity authority</td><td>A security assessment is required if providing personal information overseas.</td></tr>
<tr><td>Personal information processors who fails to meet quantity requirement specified by the national cybersecurity authority</td><td>When providing personal information overseas, two approaches are required: (1) Filing and Concluding the Standard Contract for the Outbound Transfer of Personal Information; or (2) Obtaining the Personal Information Protection Certification.</td></tr>
</table>

Table 1: Three Outbound Cross-Border Data Transfer Routes

The recently implemented ***the Regulations on Cross-border Data Flow*** further specify the applicable details of the above compliance routes.

1. If the data to be transferred outside the Chinese mainland meets the exemptions specified in Articles 3, 4, 5, and 6 of ***the Regulations on Cross-Border Data Flow*** (hereinafter referred to as "exemptions"), the enterprise can freely conduct outbound data transfer activities in accordance with the law and regulations. (For detailed content, please refer to "Part 1 Fundamentals: V. Under What Scenarios can Data be Transferred outside the Chinese mainland without Following the Three Routes of Outbound Cross-Border Data Transfer?") If the data outbound transfer does not meet the exemptions, please refer to 2-4 below for further determination.

2. If the enterprise is a Critical Information Infrastructure Operator (CIIO), it must submit the Outbound Cross-Border Data Transfer Security Assessment

of its personal information or important data to the national cybersecurity authority through the provincial cybersecurity authority where it is located.

3. If the enterprise is a data processor other than a CIIO, the first step is to determine whether the data to be transferred outside the Chinese mainland constitutes important data based on notifications or public announcements from relevant departments or regions. If the outbound data is classified as important data, the enterprise must submit the Outbound Cross-Border Data Transfer Security Assessment.

4. If the enterprise is a data processor other than a CIIO and the data to be transferred outside the Chinese mainland is personal information, then:

    i. If the enterprise has cumulatively provided personal information of over 1,000,000 individuals (excluding sensitive personal information) or sensitive personal information of over 10,000 individuals outside the Chinese mainland since January 1st of the current year, it must submit the Outbound Cross-Border Data Transfer Security Assessment.

    ii. If the enterprise has cumulatively provided personal information of over 100,000 but less than 1,000,000 individuals (excluding sensitive personal information)， or provided sensitive personal information of less than 10,000 individuals outside the Chinese mainland since January 1st of the current year, it must either conclude the Standard Contract for the Outbound Transfer of Personal Information or obtain the Personal Information Protection Certification.

For better understanding, enterprises can refer to the following flow chart for outbound data transfer systems in Figure 1 and the applicable circumstances of outbound data transfer systems in Table 2.

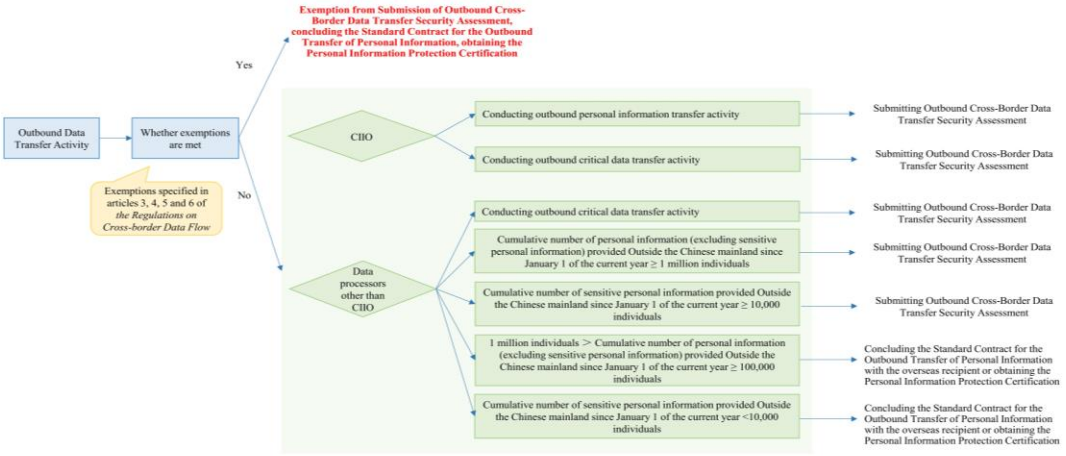


Figure 1 Flow chart of the outbound cross-border data transfer compliance route

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="4">Number of individuals involved</th></tr>
<tr><th>Subject</th><th>Data Type</th><th><10,000</th><th>≧10,000, <100,000</th><th>≧100,000, <1,000,000</th><th>≧1,000,000</th></tr>
<tr><td rowspan="2">CIIO</td><td>Important data</td><td colspan="4">Outbound Cross-Border Data Transfer Security Assessment Submission</td></tr>
<tr><td>Personal information</td><td colspan="4">Outbound Cross-Border Data Transfer Security Assessment Submission</td></tr>
<tr><td rowspan="3">Personal Information Processors other than CIIOs</td><td>Important data</td><td colspan="4">Outbound Cross-Border Data Transfer Security Assessment Submission</td></tr>
<tr><td>Sensitive personal information</td><td>conclude the Standard Contract for the Outbound Transfer of Personal Information or obtain the Personal Information Protection Certification</td><td colspan="3">Outbound Cross-Border Data Transfer Security Assessment Submission</td></tr>
<tr><td>General personal information withoutsensitive personal</td><td colspan="2">Exemption from declaration of Outbound Cross-Border Data Transfer Security Assessment, conclusion of the Standard Contract for the Outbound</td><td>conclude the Standard Contract for the Outbound Transfer of Personal</td><td>Outbound Cross-Border Data Transfer Security Assessment</td></tr>
</table>

		Number of individuals involved			
Subject	**Data Type**	**<10,000**	**≧10,000，<100,000**	**≧100,000，<1,000,000**	**≧1,000,000**
	information	Transfer of Personal Information, and certification of personal information protection		Information or obtain the Personal Information Protection Certification	Submission

Table 2 the Applicable circumstances of outbound data transfer systems

V. Under What Scenarios can Data be Transferred outside the Chinese mainland without Following the Three Routes of Outbound Cross-Border Data Transfer?

Articles 3, 4, 5 and 6 of ***the Regulations on Cross-Border Data Flow*** clearly set out the exemptions from submitting outbound cross-border data transfer security assessment, concluding a standard contract for outbound cross-border transfer of personal information, and obtaining a personal information protection certification.

1. Cross-Border Transfer of Personal Information

According to Article 4 of ***the Regulations on Cross-Border Data Flow***, if personal information collected and generated outside the Chinese mainland is transferred within the Chinese mainland to process and transferred outside the Chinese mainland later, and if the processing does not involve any domestic personal information or important data, outbound data transfer system is no longer required. For example, a domestic e-commerce platform has logistics warehouses outside the Chinese mainland and co-operates with logistics companies and airlines outside the Chinese mainland. When an overseas consumer purchases goods on the platform's international site, the merchant on the platform is responsible for organising and shipping the goods, overseas logistics enterprise and foreign airlines are operating carriers, transporting the goods and delivering them to the consumer.

Under this senario, the domestic e-commerce platform, the merchants on the

platform, the logistics enterprise, and the airlines process consumers' personal information. The order information of overseas consumers is collected by the international site and transferred back within the Chinese mainland, while the user accounts are operated and managed by the international platform, the collection of personal information of overseas consumers does not take place within the Chinese mainland, and the no domestic personal information is involved in the data process. The order information of the transaction is confirmed by the platform and then sent to the overseas logistics enterprise and the airlines to transport and deliver the goods.

Therefore, according to Article 4 of ***the Regulations on Cross-Border Data Flow***, for the above scenario, the e-commerce platform does not need to adopt an additional outbound data transfer system. This improves the efficiency of cross-border e-commerce.

2. Where it is necessary to provide employees' personal information outside the Chinese mainland for cross-border human resources management

According to subparagraph 2 of paragraph 1 of Article 5 of ***the Regulations on Cross-Border Data Flow***, if there is a genuine need to provide employees' personal information outside the Chinese mainland for the purpose of conducting cross-border human resources management in accordance with the employment rules and regulations formulated in accordance with the law, and collective contracts concluded in accordance with the law, there is no need to adopt an additional outbound data transfer system. However, if an enterprise wishes to be exempted from adopting the outbound data transfer system based on this scenario, it must ensure that the the cross-border transfer of employee's personal information is "genuinely necessary" for the implementation of human resources management. The enterprise must also ensure that the cross-border transfer of specific fields is also "genuinely necessary" for the implementation of human resources management.

3. Where it is necessary to provide personal information outside the Chinese mainland for the purpose of concluding or performing a contract

According to subparagraph 1 of paragraph 1 of Article 5 of ***the Regulations on Cross-Border Data Flow***, if it is necessary to provide personal information abroad to meet the requirement of "being essential for the conclusion or performance of a contract to which the individual is a party", no additional outbound data transfer systems are

required. This Article identifies the scenarios where it is "necessary for the performance of a contract", such as cross-border shopping, cross-border delivery, cross-border remittance, cross-border payment, cross-border account opening, air ticket and hotel booking, visa application, examination services, and other scenarios that require the provision of personal information outside the Chinese mainland. For example, when a consumer invests in an international financial product, in order to meet the requirements of the contract, legal provisions or industry regulatory requirements, they must provide personal information outside the Chinese mainland, such as the investor's name, ID card information, contact information, financial status, etc..

4. Where it is necessary to provide personal information outside the Chinese mainland in an emergency to protect the life, health and property safety of a natural person.

According to subparagraph 3 of paragraph 1 of Article 5 of ***the Regulations on Cross-Border Data Flow***, if there is a genuine need to provide personal information outside the Chinese mainland "in order to protect the life, health and property safety of natural persons in emergency scenarios, etc.", there is no need to adopt an additional outbound data transfer system. For example, in the event of a sudden outbreak of an epidemic in a certain country, in order to save the lives of the affected people, certain organisations may need to send the personal information of the patients to international relief agencies. This allows the agencies to promptly determine the cause of the outbreak, access whether the outbreak has already occurred in other countries or regions,confirm the degree of similarity, supply medicines to the affected areas, and to take the necessary relief measures. The purpose of this article is to ensure the rational allocation of relief resources and the safety of people's lives.

5. International trade

According to Article 3 of ***the Regulations on Cross-Border Data Flow***, the outbound transfer of data collected and generated in international trade activities that do not contain personal information or important data does not require the adoption of an additional outbound data transfer system. For example, when a domestic foreign trade enterprise exports goods to another country, it needs to send information on the quantity, specifications, weight, value and mode of transport of the goods to the importing party, enabling customs, logistics companies and trading partners in various

countries to manage the transport and delivery of the exported goods. But the concept of "international trade" is very broad. Questions such as what types of commercial activities fall within the scope of "international trade", what processes in practice fall within the scope of "international trade", and whether the recipients of overseas data are limited to trading partners, need to be further explained.

6. Cross-Border Transport

According to article 3 of ***the Regulations on Cross-Border Data Flow***, the outbound transfer of data collected and generated during cross-border transport activities that do not contain personal information or important data does not require the adoption of an additional outbound data transfer system. For example, it is relatively common that a domestic consumer purchases goods from an overseas merchant on an e-commerce platform, where the merchant's place of shipment is located outside the Chinese mainland. The goods need to be transported across the border from outside of the country to the country, and this process may involve the platform party providing personal information, such as the domestic consumer's receiving address and contact information, to the international carrier outside of the country to complete the cross-border transport of the goods.

However, similar to Scenario 5, the concept of "cross-border transport" is broad. It encompasses not only the transportation of goods related to routine-commerce platform transactions, but also more complex transport scenarios, such as the international long-distance shipment of non-retail bulk commodities, including ore resources, agricultural products, crude oil, and so on. Whether all these scenarios can be included in the scope of the exemption remains to be further explored in practice.

7. Academic Cooperation

According to article 3 of ***the Regulations on Cross-Border Data Flow***, general cross-border data transfer activities that do not contain personal information or important data collected and generated in the course of academic cooperation activities do not require the adoption of an additional outbound data transfer system. For example, a research institute of a domestic university cooperating with researchers from other countries or institutions may need to share data, such as experimental results, survey conclusions, statistical data that do not contain personal information or important data. Cross-border transfer of academic-related data can promote international academic co-

operation and exchanges, facilitating the development of global scientific research.

However, similar to Scenario 5, the applicability of the industry sectors of academic cooperation scenarios is broad. Even if the data in certain industry sectors do not constitute personal information or important data, large-scale statistical data or sensitive data may constitute “intelligence”, “state secrets”, and etc. Identifying whether the academic data to be shared in an academic co-operation scenario involves important data or state secrets is a highly technical. Therefore, special care should be taken in applying the exemption provisions in such scenarios, in order to prevent scenarios that may jeopardise national security and the interests of society.

8. Transnational Manufacturing

According to article 3 of ***the Regulations on Cross-Border Data Flow***, general data outbound transfer activities that do not contain personal information or important data collected and generated in the course of transnational production and manufacturing activities are likewise not subject to an additional outbound data transfer system. For example, a state-owned enterprise in the manufacturing industry has production bases in a number of countries around the world. When manufacturing and assembling its products, in order to conduct effective supply chain management of the global production bases and to ensure the timely supply of materials, data involving material inventory management information, parts and components production schedules, and logistic and transport information need to be provided to the overseas bases.

However, similar to scenario 5, the concept of “cross-border manufacturing” is broad and involves more links, cumbersome procedures, and a variety of participants, making the chain of data exit relatively complex. Therefore, enterprises need to further explore the compliance standards in practice, and are also advised to communicate with regulators on “suspicious issues” in a timely manner.

9. Transnational Marketing

According to article 3 of ***the Regulations on Cross-Border Data Flow***, general data outbound transfer activities that do not contain personal information or important data collected and generated in the course of cross-border marketing activities do not require the adoption of additional outbound data transfer system. For example,

multinational consumer goods enterprises will conduct research on the domestic market before they enter the Chinese market or expand their business in the Chinese market. For this purpose, the enterprise will inevitably need to collect and analyse a number of market data, including market research reports on various lines of China's market, peer market share analysis data, consumer behaviour data, to fully understand consumer demand, competition and market trends in the target market.

By collecting relevant domestic market data, the multinational enterprise can better understand and grasp the characteristics and opportunities of the target market in China, and formulate corresponding marketing strategies and plans. This approach supports the enterprise's marketing decisions and promotional activities in China and further promote China's economic development.

10. Other general data

In addition to the various scenarios listed in Scenarios 5 to 9, Article 3 of ***the Regulations on Cross-Border Data Flow*** provides an underpinning nature for general data that does not contain personal information or important data in - i.e., in the activities of international trade, cross-border transport, academic cooperation, cross-border production and manufacturing and marketing, no additional outbound data transfer system is required. However, are general data under all similar activities free to flow across borders? How to determine the specific scope of "activities and etc."? How can other activities in practice be exempted from the provisions of Article 3 by analogy? These details need to be further clarified in the light of examples of regulatory practice.

11. "FTA Negative List" Data

In addition to explicitly mentioning the above ten scenarios, ***the Regulations on Cross-Border Data Flow*** also specifically design a special mechanism of the Negative List.Under the framework of the national data classification and hierarchical protection system, the FTZs may formulate on their own the list of data that need to be included in the scope of data outbound security assessment, standard contract for the outbound transfer of personal information, personal information protection certification and management in the FTZs. The list must be submitted for approval by the provincial cyberspace administration , and then reported to the CAC and the national data administration for record. Data processors in the FTZs that provide data outside the

Negative List to foreign countries are exempted from dfiling a security assessment for providing data abroad, entering a standard contract for providing personal information abroad or obtaining authentication for personal information protection.

VI. Which Scenarios Fall under the Category of "Laws and Administrative Regulations Provide Otherwise, and Assessment/Approval Shall be Submitted in Accordance with Their Provisions"?

In addition to the overall system of data and network security established by ***the Cybersecurity Law***, ***the Data Security Law*** and ***the Personal Information Protection Law***, enterprises should also consider the requirements of other relevant laws and regulations. For example, according to article 37 of ***the Law of the People's Republic of China on the Preservation of State Secrets***, if an organ or unit provides State secrets to foreign countries or to organizations or institutions set up by foreign countries within the territory of China, or if it appoints or employs personnel from abroad who are required to know State secrets for the purpose of their work, the matter shall be processed in accordance with the relevant State regulations. Under the provisions of article 42, organs and units procuring goods and services involving State secrets, and units engaged in the construction, design, building and supervision of projects directly involving State secrets, shall abide by the provisions on State secrecy. Where an organ or unit entrusts an enterprise or institution to engage in business involving State secrets, it shall enter into a confidentiality agreement with the vendor, making confidentiality requirements and taking confidentiality measures.

If healthcare big data is involved, it shall be stored on a safe and trustworthy server within the country in accordance with Article 30 of ***the Measures for the Management of National Healthcare Big Data Standards, Security and Services (for Trial Implementation)***.If it is necessary to provide it outside of the country due to business needs, it shall be subject to security assessment and review in accordance with relevant laws and regulations and relevant requirements.

If the results of surveying and mapping are involved, according to Article 34 of ***the Surveying and Mapping Law of the People's Republic of China***, if they are state

secrets, the provisions of laws and administrative regulations on confidentiality shall apply; if they need to be made available to the outside world, they shall be implemented in accordance with the examination and approval procedures stipulated by the State Council and the Central Military Commission.

If information on human genetic resources is involved, in accordance with article 57 of ***the Biosafety Law of the People's Republic of China***, if it is to be made available to, or open for use by, foreign organisations or individuals and institutions established or under their actual control, a prior report shall be made to the competent department of science and technology under the State Council and a back-up copy of the information shall be submitted.

VII. Which Scenarios Fall under the Category of "Laws and Administrative Regulations Provide Otherwise, and Assessment/Approval Shall be Submitted in Accordance with Their Provisions"?

The Regulations on Cross-border Data Flow have moderately narrowed the scope of the outbound cross-border data transfer security assessment. According to ***the Regulations on Cross-border Data Flow*** and ***the Guidelines to Assessment Submission (Second Edition)***, when outbound data transfer activities do not fall under the exemption scenarios specified in ***the Regulations on Cross-border Data Flow*** (For detailed content, please refer to "Part 1 Fundamentals: V. Under What Scenarios can Data be Transferred outside the Chinese mainland without Following the Three Routes of Outbound Cross-Border Data Transfer?"), and if any of the following scenarios apply, data processors must submit the Outbound Cross-Border Data Transfer Security Assessment:

1. CIIO providing personal information or important data outside the Chinese mainland;
2. Data processors other than CIIO providing important data outside the Chinese mainland;
3. Data processors other than a CIIO providing personal information of over

1,000,000 individuals (excluding sensitive personal information) outside the Chinese mainland since January 1st of the current year;

4. Data processors other than a CIIO providing sensitive personal information of over 10,000 individuals to foreign entities outside the Chinese mainland since January 1st of the current year.

Meanwhile, Article 6 of ***the Regulations on Cross-border Data Flow*** stipulates that pilot free trade zones, within the framework of the national data classification and grading protection system, can issue a specific data list (hereinafter referred to as the negative list) which regulates the outbound cross-border data transfer security assessment, standard contract for the outbound transfer of personal information , and personal information protection certification. This list must be approved by the provincial cybersecurity and informatization committee and then submit to the national cybersecurity authority and the national data management department for filing. Data processors within the pilot free trade zones, when transfering outbound data not in the negative list, are exempted from applying for a outbound cross-border data transfer security assessment, concluding a standard contract for the outbound transfer of personal information , or obtaining personal information protection certification.

VIII. What is the Procedure of Outbound Cross-Border Data Transfer Security Assessment?

To better help data processors to submit outbound cross-border data transfer security assessment, the national cybersecurity authority, based on practical experience, has issued ***the Guidelines to Assessment Submission (Second Edition)***. The guideline simplifies the requirement for submission documents and a *Outbound Data Transfer Submission System* is launched at the same time.

According to ***the Guidelines to Assessment Submission (Second Edition)***, the submission for outbound cross-border data transfer security assessment can be submitted both online and offline:

Online submission is generally applicable to data processors other than CIIO. When data processors other than CIIO have cumulatively provided personal information of over 1 million individuals (excluding sensitive personal information)

outside the Chinese mainland since January 1st of the current year, they need to submit a outbound data transfer security assessment.

Offline submission is usually applicable to CIIO or other entities that are not suitable for submitting through the online system. However, the specific scenarios where it is "not suitable to apply for outbound data cross-border transfer security assessment through the online system" still need further clarification by the cybersecurity authority.

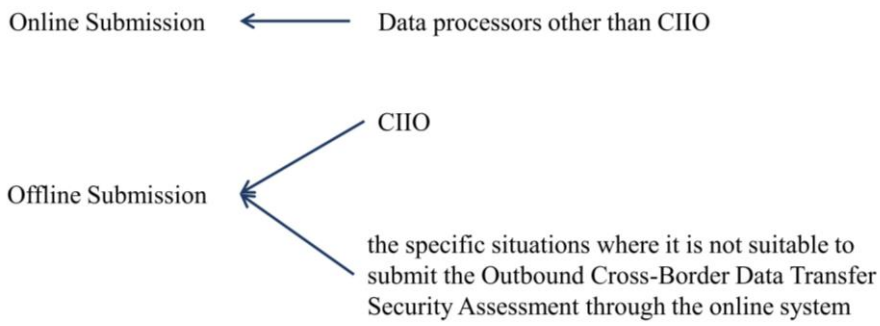


Figure 2 The Applicable scope of different security assessment submission procedure

（一）线上申报流程

1. Online Submission

Data processors shall submit outbound data transfer submission materials through the online Data Export Submission System at https://sjcj.cac.gov.cn. According to ***the Instructions for Outbound Data Transfer Submission System (First Edition)***, the system integrates the submission process for both outbound cross-border data transfer security assessments and the filing of standard contracts for outbound personal information transfer. The online filing system will support personal information protection certification in the future, but the relevant functionality is still under development and has not yet been launched. Currently, enterprises can apply for personal information protection certification through the Personal Information Protection Certification Management System at [7].

[7] See CAC, Q&A on Provisions on Promoting and Regulating Cross-Border Data Flow , https://mp.weixin.qq.com/s/-Y-

Before formally submitting an assessment, data processors should prepare the following documents in accordance with Article 3 of ***the Guidelines to Assessment Submission (Second Edition)*** and ***the Instructions for Outbound Data Transfer Submission System (First Edition)***:

- A photocopy of the Uniform Social Credit Code certificate (with official seal)
- A photocopy of the legal representative's identification document (with official seal)
- A photocopy of the authorized agent's identification document (with official seal)
- Authorization Letter and Commitment Letter from the authorized agent
- Outbound data transfer security assessment submission form
- Photocopies of outbound data transfer contracts or other legally binding documents (with official seal)
- Scanned copy of the outbound data transfer risk self-assessment report

Once the above documents are prepared, data processors should use the Outbound Data Transfer Submission System to submit a outbound data transfer security assessment by following these steps: "Register a user account → Configure the system usage environment → Select the new assessment entry".

1. During the account registration, data processors should have prepared scanned copies or photos of the Uniform Social Credit Code certificate, legal representative's identification, system registrant's identification, and the registration authorization letter. If the entity making the submission is an individual, they can select "No Legal Representative Information" to skip this step and proceed with the subsequent entries.
2. During the system usage environment configuration stage, data processors can choose from three user authentication methods based on their actual scenarios: SMS authentication, a professional browser combined with a soft

dY_HL21jHTFQsMbeiVQ.

certificate for authentication, or Ukey authentication.

3. Click on "Outbound Data Transfer Security Assessment Management". Select "New Assessment" to enter the new assessment submission page. Then, uploading the security assessment documents and, after entering the wizard page, please follow the prompts to gradually complete the submission information, including the following steps:

    - Checking whether the data transfer activities fall under the scope for outbound data transfer security assessment submission.
    - Filing in the data processors' information.
    - Entering the legal representative's information.
    - Providing the data protection officer and management organization details.
    - Filling in the authorized agents information.
    - Specifying the data processor's compliance with Chinese laws, administrative regulations, and departmental rules.
    - Describing the outbound data transfer scenario.
    - Uploading other relevant materials for the data export security assessment submission.

2. Offline Submission

CIIO or other entities that are not suitable for submitting security assessment through the online system should use the offline system to submit their submission to the national cybersecurity authority via the provincial cybersecurity authority where they are located. According to ***the Guidelines to Assessment Submission (Second Edition)***, the following submission documents are needed:

- Uniform Social Credit Code certificate (stamped with the official seal)
- Legal representative's identification document (stamped with the official seal)
- The authorized agents identification document (stamped with the

official seal)

- Authorization Letter and Commitment Letter from the authorized agent
- Outbound data transfer security assessment submission form
- Outbound data transfer contracts or other legally binding documents (stamped with the official seal)
- Outbound data transfer risk self-assessment report
- Others

IX. How long will Outbound Data Transfer Security Assessment Submission Take?

The Guidelines to Assessment Submission (Second Edition) does not differentiate the timeline between online submission and offline submission. Generally, the submission timeline for an outbound data transfer security assessment is shown in Figure 3:

Figure 3 the Submission Timeline for an Outbound Data Transfer Security Assessment

According to Article 2 of ***the Guidelines to Assessment Submission (Second Edition)***, the provincial cybersecurity authority will complete a completeness check within 5 working days of receiving the submission materials and will inform the data processors of the results. For submission that pass the completeness check, the provincial cybersecurity authority will submit the materials to the CAC for further process. For submission that do not pass the completeness check, the provincial cybersecurity authority will inform the data processors of the reasons for the failure.

The CAC will, within 7 working days of receiving the submission materials submitted by the provincial cybersecurity authority, decide whether to accept the submission and will notify the data processor in writing. According to Article 12 of ***the Assessment Measures for Data Transfer***, the CAC will complete the outbound data transfer security assessment within 45 working days from the date the written acceptance notice is issued to the data processor.

During the overall assessment, if the case is complicated, additional documents are needed or documents needed to be corrected, the CAC may extend the assessment period accordingly and will inform the data processors of the estimated extension time. If the processor fails to supply or modify the submission materials without a valid reason, the CAC may terminate the security assessment. Once the assessment is completed, the CAC will issue an assessment result notice to the data processor. The data processor must regulate its outbound data activities in accordance with the relevant laws, regulations, and the requirements stated in the assessment result notice. If the data processor disagrees with the assessment results, they can re-submit an assessment within 15 working days of receiving the assessment result notice. The reassessment result will be final.

X. Under What Scenarios Can an Enterprise Choose to Conclude and File the Standard Contract for the Outbound Transfer of Personal Information?

The Regulations on Cross-Border Data Flow appropriately ease the restrictions on cross-border data transfer and adjust the requirements for concluding standard contract for cross-border transfer of personal information. Specifically, according to ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***, an enterprise that meets the following scenarios simultaneously and does not fall into the exemptions under ***the Regulations on Cross-Border Data Flow,*** (For detailed content, please refer to "Part 1 Fundamentals: V. Under What Scenarios can Data be Transferred outside the Chinese mainland without Following the Three Routes of Outbound Cross-Border Data Transfer?") can choose to and file a standard contract:

1. Data processors other than CIIO;

2. The cumulative number of personal information transferred outside the Chinese mainland is more than 100,000 and less than 1,000,000.00 individuals (excluding sensitive personal information) since January 1st of the current year;

3. The cumulative number of sensitive personal information transferred outside the Chinese mainland is less than 10,000 individuals since January 1st of the current year.

It should be noted that if personal information intended to be transferred outside the Chinese mainland has been announced or published as important data by relevant departments or regions, the enterprise shall submit the outbound cross-border data transfer security assessment rather than concluding the standard contract for outbound cross-border transfer of personal information or obtaining the personal information protection certification.

XI. What is the Process of Concluding and Filing the Standard Contract for the Outbound Cross-Border Transfer of Personal Information?

To help personal information processors in filing the standard contract for cross-border transfer of personal information, the CAC has published ***the Guidelines to Recording Submission of Standard Contract (Second Edition)*** based on its previous experience in filing. ***The Guidelines to Recording Submission of Standard Contract (Second Edition)*** has modified and optimized the requirements to conclude the standard contract, including the scope of submission, filing methods, filing process, and required materials. It also provides the contact information for consulting and reporting.

The process of filing the standard contract can be summarized as "submitting the Personal Information Protection Impact Assessment and concluding the contract → submitting materials → materials inspection and feedback on the filing results → submitting supplementary materials or re-filing the standard contract → completing the filing of the standard contract → conducting the cross-border transfer of personal information." The timeline and process are illustrated in Figure 4 below:

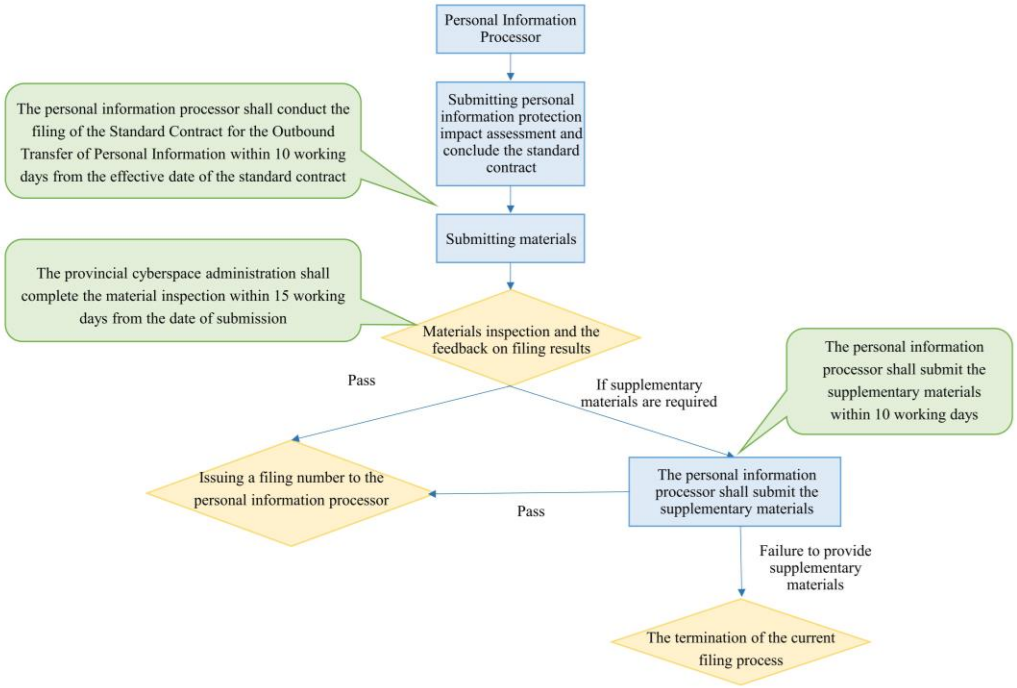


Figure 4 Filing the Standard Contract for the Outbound Transfer of Personal Information

The procedure of filing the standard contract for the outbound cross-border transfer of personal information is as follows:

1. Submitting the Personal Information Protection Impact Assessment and concluding the contract

First, the personal information processor shall submit the Personal Information Protection Impact Assessment before filing the standard contract for the cross-border transfer of personal information. Article 55 of ***the Personal Information Protection Law*** and Article 5 of ***the Measures for the Standard Contract*** stipulates that the Personal Information Protection Impact Assessment shall be submitted and recorded before conducting cross-border transfer of personal information.(For detailed content, please refer to "Part 2 Practice: XXX. How to Submit a Personal Information Protection Impact Assessment? ") Meanwhile, the enterprise shall submit Annex II based on its own scenario in accordance with the standard contract model issued by the CAC, and conclude the standard contract with overseas recipients.

2. Submitting materials

As the filing process has been changed from offline to online, the personal

information processor shall, in accordance with Article 7 of ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***, file the standard contract for cross-border transfer of personal information through the Cross-Border Data Transfer Filing System, which is available at, within 10 working days from the effective date of the standard contract. According to ***the Instructions for Outbound Data Transfer Submission System (First Edition)***, the personal information processor using the Cross-Border Data Transfer Filing System shall follow the process of "registering a user account → configuring the system's operating environment → selecting a new filing portal." These steps are required for filing of the standard contract for cross-border transfer of personal information.

The specific operational processes and requirements for registering user account and configuring the system's operating environment are the same as those for filing cross-border data transfer security assessment.(For detailed content, please refer to "Part 1 Fundamentals: VIII. What is the Procedure of Outbound Cross-Border Data Transfer Security Assessment?")

After logging into the system, the data processor should select "New Filing" to file the standard contract for the cross-border transfer of personal information. According to ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***, and ***the Instructions for Outbound Data Transfer Submission System (First Edition)***, the data processor shall submit the following documents for filing the standard contract for cross-border transfer of personal information:

- Photocopy of certificate for unified social credit code
- Photocopy of the identification card of the legal representative
- Photocopy of the identification card of the authorized agent
- Authorization letter from the authorized agent
- Photocopy of the signed and sealed commitment letter
- Photocopy of the Standard Contract for Cross-Border Transfer of Personal Information (with official seal)
- Photocopy of *Personal Information Protection Impact Assessment Report* (with official seal)

The enterprise should submit the following materials following the instructions in the Cross-Border Data Transfer Filing System, including:

- Confirming the applicable scenarios of the standard contract for outbound cross-border transfer of personal information
- Filling in the basic information of the personal information processor
- Filling in the information of the legal representative
- Filling in the information of the authorized agent
- Uploading the photocopy of the signed and sealed commitment letter
- Filling in the situation of the personal information processor's compliance with Chinese laws, administrative regulations, and departmental rules
- Filling in the scenario of cross-border transfer of personal information
- Uploading a photocopy of the Standard Contract for Cross-Border Transfer of Personal Information (with official seal) and fill in relevant information
- Uploading a photocopy of the *Personal Information Protection Impact Assessment Report* (with official seal)
- Uploading other relevant supporting documents.

3. Materials inspection and the feedback on filing results

After submitting the materials, enterprise shall wait for the materials check and the feedback of filing results. According to Article 3 of ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***, the provincial cyberspace administration shall complete the material check within 15 working days from the date of submission, and issue a filing number to the personal information processor that meets the filing requirements. If supplementary materials are required, the personal information processor shall submit the supplementary materials within 10 working days. Failure to provide supplementary materials within the due time may result in the termination of the current filing process.

XII. Under What Scenarios Can an Enterprise Choose to Obtain the Personal Information Protection Certification?

Processors of personal information may determine whether they are subject to the Personal Information Protection Certification Pathway based on the following three questions :

(1) In terms of exemptions: are they among the six situations exempted from the three major data outbound compliance paths in *the Regulations on Cross-border Data Flow*?

(2) In terms of the outbound subject: is it a CIIO?

(3) In terms of the type and quantity of outbound data: does the outbound data involve important data? Does the outbound personal information involve more than one million individuals? Does the outbound sensitive personal information involve more than 10,000 individuals?

If all of answers to the above questions are “no” and “the accumulated personal information (excluding sensitive personal information) of more than 100,000 individuals but less than 1 million individuals or less than 10,000 individuals of sensitive personal information has been provided outside the Chinese mainland since January 1 of the current year”, then the processor of personal information will be in a position to comply with the three major outbound data transfer compliance requirements. ITherefore, the personal information processor can choose to obtain the outbound personal information protection certification or conclude the standard contract.

At the same time, standard contract filing and outbound personal information protection certification,as parallel compliance paths, have made the choice of appropriateness a primary concern for personal information processors . In view of the significant differences between the two in terms of the subject of application, validity period, audit mechanism and state supervision, enterprises should refer to the following two paths for a comprehensive assessment of the characteristics of the enterprise's personal information outbound according to the specific circumstances of the enterprise, and choose the compliance program that best meets the actual needs.

	Personal Information Protection Certification	Filing and Concluding the Standard Contract
Subject of application or filing	Both domestic and overseas personal information processors can apply for personal information protection certification for outbound personal information transfer activities.	The subject of the record must be the same as the subject of the standard contract signed within the Chinese mainland.
validity period	3 years	Agreed by the contract parties
Subject of audit	Professional Certification Bodies	Provincial Cyberspace Administration
Application Process	Certification application, technical validation, on-site audit, certification decision, continuous monitoring	Filing application, material inspection, result feedback, supplement or re-filing
State supervision	1. If the certification body finds that the rights and interests of personal information are seriously affected, it shall promptly report to the national cyberspace authority and relevant departments; 2. The municipal supervisory department and the national cyberspace authority shall conduct random checks on the certification process and certification results.	Both parties fulfill their obligations to protect personal information in accordance with the terms and conditions of the standard contract, and at the same time, they are required to submit the signed contract and the impact assessment report on the protection of personal information to the national cyberspace authority for record.

In addition, it should be clarified that the provision of personal information outside the Chinese mainland that has been notified or publicly released as important data by the relevant department or region shall be declared as an Outbound Cross-Border Data Transfer Security Assessment, and the option of filing and concluding the Standard Contract for the Outbound Transfer of Personal Information or obtaining the Personal Information Protection Certification shall not be available.

XIII. What is the Process of Obtaining a Personal Information Protection Certification?

On November 18 2022, the State Administration for Market Supervision and Administration and the CAC issued the Certification Announcement and the annexed Certification Rules, which provide details of the process of obtaining personal

information protection certification, including certification entrustment, technical verification, on-site auditing, evaluation of certification results, and approval. The Certification Announcement states that "certification institutions engaged in the certification of personal information protection shall have obtained approval before issuing relevant certifications".

Although the relevant laws and regulations do not explicitly publish a list of qualified certification institutions in accordance with the law, consultation results with the China Cybersecurity Review, Certification, and Market Regulation Big Data Center (hereinafter referred to as the **Big Data Center**), as well as *the Answer to Reporter's Question on* ***the Provisions of Regulations on Cross-Border Data Flow*** issued by the CAC on March 22, 2024, indicate that enterprises can apply to the Big Data Centre through the Personal Information Protection Certification Management System (specifically at https://data.isccc.gov.cn) (For detailed content, please refer to "Part 2 Practice: XL. To whom should the Application of Personal Information Protection Certification be Submitted? ").

At the same time, ***the Certification Requirements for Cross-Border Transfer (Draft)*** specify the applicable scenarios, basic principles, and basic requirements for obtaining personal information protection certification in the context of cross-border personal information transfer. These requirement provide a certification basis for certification institutions to conduct personal information protection certification of cross-border processing activities. Additionally, they serve as a reference for enterprises to conduct cross-border processing of personal information as personal information processors in a compliant manner.

The certification of personal information protection includes five steps: "certification entrustment, technical verification, on-site audit, evaluation and approval of certification results, and post-certification supervision", and the specific process is shown in Figure 5:

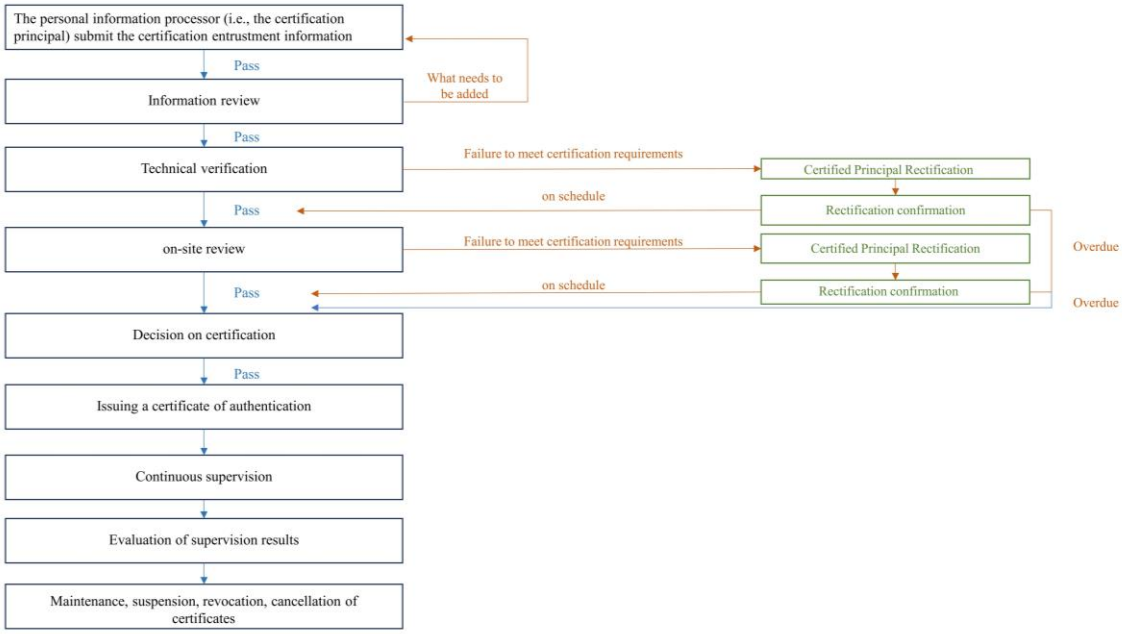


Figure 5 Flow Figure of Personal Information Protection Certification Process

Combined with ***the Certification Measures for Outbound Personal Information Transfer (Draft)***, we summarize the action plan of the certification applicant and the certification institute in the whole process of certification, as shown in the table below:

Certification Process	Certification Applicant To do	Certification Institute To do
1.Accreditation commission	(1) Pre-application rectification: Before applying for personal information protection certification, self-assessment and compliance rectification can be carried out in accordance with the requirements of the certification basis, in order to meet the relevant requirements of the certification basis. (2) Submission of Certification Entrusted Data: The personal	(1) Notification of acceptance or not: The certification institute provides timely feedback on whether or not it is acceptable after reviewing the certification entrusted information. (2) Confirmation of the certification program and notification: the certification body determines the certification program based

Certification Process	Certification Applicant To do	Certification Institute To do
	information processor (i.e., the certification principal) submits the certification entrusted data, including but not limited to the basic materials of the certification principal, the certification entrustment letter, and relevant supporting documents.	on the certification entrusted information, including the type and quantity of personal information, the scope of personal information processing activities involved, and information on the technical verification organization, etc., and notifies the certification entrusted person.[8]
2. Technical verification	Actively cooperate with the technical certification body to implement technical certification in accordance with the certification program, and receive the technical certification report.	Issuance of a technical validation report[9].
3. On-site audit	Actively cooperate with the certification body to implement on-site audits, and receive on-site audit reports.	Implementation of on-site audit, and issuedon-site audit report to the certification commissioner [10].
4. Evaluation and approval of accreditation	/	(1) certification decision: a certification decision is made based on the certification commission information, technical verification reports,

[8] See Article 4.1 of the Certification Rules.
[9] See Article 4.2 of the Certification Rules.
[10] See Article 4.3 of the Certification Rules.

Certification Process	Certification Applicant To do	Certification Institute To do
results		on-site audit reports and other relevant information information for a comprehensive evaluation
	Receive certificates of accreditation.	a. Certificates of accreditation shall be issued for compliance with the requirements for accreditation;
	Make corrections according to the requirements of the certification institute and re-submit the certification materials=.	b. For the time being does not meet the certification requirements, the certification commissioner is required to rectify the deadline; for rectification is still not in line with the written notification of the certification commissioner to terminate the certification.
	No deception, concealment of information, or willful violation of certification requirements shall be committed.	c. If it is found that the certification applicant or personal information processor has behaviors that seriously affect the implementation of certification, such as deception, concealment of information, and intentional

Certification Process	Certification Applicant To do	Certification Institute To do
		violation of certification requirements, the certification will not be issued.
	/	(2) report the results of certification: within five working days after the issuance of certification, to the national certification and accreditation of public information platform to report personal information out of the personal information protection certification information, including the certification certificate number, the name of the certified personal information processor, the scope of the certification and certificate status change information.
5. Post-licensing monitoring	Ensure that the activities of cross-border transfer of personal information continue to comply with the certification requirements, then the certificate of certification may be continued; otherwise, suspension up to revocation of the certificate of	(1) Ongoing supervision: Within the validity period of the certification (3 years), the certified personal information processor shall be subject to ongoing supervision, and the frequency of supervision shall be reasonably determined.

Certification Process	Certification Applicant To do	Certification Institute To do
	certification may be imposed.	(2) Make evaluation conclusions: Comprehensive evaluation of the post-certification supervision conclusions and other relevant data and information; if the evaluation passes, the certification may be continued; if it fails, the certification shall be suspended or revoked in accordance with the corresponding circumstances.
6. Renewal of certificates of accreditation	The expiration of the certificate needs to continue to use, should be in the expiration of the validity of six months before the certification commission.	Adopting a post-certification monitoring approach to commission new certificates for those that meet certification requirements.
7. Changes to certificates of accreditation	(1) Submit a change commission: If the name or registered address of the certified personal information processor, or the certification requirements or the scope of certification change during the validity period of the certification, a change commission shall be submitted to the certification body.	(1) Confirmation of the content of the change: Based on the content of the change, the change commissioning information shall be evaluated to determine whether the change can be approved. (2) technical verification and / or on-site audit: If the need for

Certification Process	Certification Applicant To do	Certification Institute To do
	(2) Cooperate with technical verification and/or on-site audit (if required).	technical verification and / or on-site audit, should also be approved before the change in technical verification and / or on-site audit. (3) report the results of certification: within five working days after the certification status changes to the national certification and accreditation of public information platform to report personal information out of the country personal information protection certification certificate-related information.
8. Cancellation, suspension and revocation of accreditation certificates	In the validity of the certificate, the applicant can apply for certificate suspension and cancellation.	When it is found that a certified personal information processor no longer meets the certification requirements, such as when the exit of personal information is inconsistent with the scope of certification, the certificate of certification shall be suspended or revoked in a timely manner and shall be made public.

XIV. What are the CIIO Outbound Data Transfer Requirements?

CIIOs, including telecom operators, financial institutions and energy suppliers, hold large amounts of personal information and important data. The security of such data is critical for both countries and individuals. For example, financial institutions process their customers' financial information, telecommunication operators process their subscribers' communication data, and energy suppliers hold critical data on energy supply and distribution. By regulating personal information and important data provided by CIIOs outside the country, it is possible to prevent these data from being misused, leaked or used for unlawful purposes.

The laws currently in force in China clearly regulate the outbound data transfer activities of CIIO. Article 37 of ***the Cybersecurity Law*** mandates that CIIOs must undergo a security assessment before providing data outside the Chinese mainland. Article 40 of ***the Personal Information Protection Law*** further stipulates that CIIOs shall store personal information collected and generated within the Chinese mainland. If it is necessary to provide such information outside the Chinese mainland, it shall pass the security assessment organised by the national cybersecurity authority.

It is evident that China has adopted a stringent approach to controlling the outbound data transfer activities of CIIOs, as the leakage, destruction, and loss of CIIO data may have a significant impact on national security, social public interests, and individual privacy.

It should be noted, however, that Article 7 of ***the Regulations on Cross-Border Data Flow***, while clarifying the conditions for CIIOs to submit Outbound Cross-Border Data Transfer Security Assessment, stipulates that "in cases falling under the provisions of Articles 3, 4, 5 and 6, the provisions shall apply as provided for in those articles". Subparagraphs 1-3 of paragraph 1 of Article 5 of ***the Regulations on Cross-Border Data Flow*** lists three scenarios under which the provision of personal information by a data processor outside the Chinese mainland is exempted from the outbound data transfer system:

(i) The provision of personal information outside the Chinese mainland for the purpose of concluding and performing a contract to which the individual is a party;

(ii) the provision of employees' personal information outside the Chinese

mainland for the purpose of implementing cross-border human resources management in accordance with labour rules and regulations formulated in accordance with the law and a collective contract concluded in accordance with the law; and

(iii) the provision of employees' personal information outside the Chinese mainland for the purpose of implementing cross-border human resources management in accordance with labour rules and regulations and collective contracts in accordance with the law; and

(iii) to provide personal information outside the Chinese mainland for the purpose of protecting the life, health and property safety of natural persons in emergency scenarios. Therefore, if a CIIO provides personal information abroad under the above three scenarios, it may be exempted from the submission of security assessment on outbound cross-border data transfer in accordance with the above provisions.

While most enterprises are not CIIOs and the impact of the above provisions is relatively small, these enterprises need to identify whether their clients or collaborators are CIIOs. Enterprises will need to comply with the compliance obligations for cross-border data interactions with CIIOs in particular when they conduct business activities with CIIOs.

XV. What are the Legal and Regulatory Bases for Identifying Important Data?

In order to ensure data security and safeguard national interests, cross-border transfer of important data has become a focus of regulatory attention in various countries and regions. China's regulatory authorities also explicitly require enterprises not only to submit risk self-assessments of the outbound transfer activities of "important data", but also to apply for security assessments of outbound data transfers to cyberspace administration authorities. This aims to strengthen the administration of outbound data transfer and ensure data security.

Article 21 of ***the Data Security Law*** provides that the national data security coordination mechanism shall make overall planning for and coordinate relevant departments in formulating the catalogues for important data and strengthening the protection of important data. In response to this requirement, the national standard

GB/T 43697-2024 Data Security Technology — Rules for Data Classification and Grading was officially released on March 15 2024. Under this standard, Article 6.5 (b) and Appendix G ***Guidelines for the Identification of Important Data*** set forth clear criteria for identifying important data at the national macro level. Data that meet any one of the following criterion will be identified as important data:

(i) if the data is leaked, tampered with, damaged or illegally obtained, used or shared, it directly poses a **general hazard** to **national security**;

(ii) if the data is leaked, tampered with, damaged or illegally obtained, used or shared, it directly poses a **serious hazard** to the **functioning of economy**;

(iii) if the data is leaked, tampered with, damaged or illegally obtained, used or shared, it directly poses a **serious hazard** to the **social order** (e.g., affecting social stability);

(iv) if the data is leaked, tampered with, damaged or illegally obtained, used or shared, it directly poses a **serious hazard** to the **public interest** (e.g., endangering public health and safety);

(v) where the data is **directly related to specific areas, groups or regions** of national security, functioning of economy, social stability, public health and safety; (vi) where the data reaches certain level of precision, scale, depth or importance, and **directly affects national security, functioning of economy, social stability, public health and safety**; and

(vi) if it is important data determined by the assessment of the competent (supervisory) authorities of the industry sector.

In addition, various local governments and governmental departments are also stepping up efforts with the establishment of specific catalogues of important data in their own regions and departments, as well as in related industries and fields, so as to provide enterprises with more comprehensively applicable and operable norms for the identification of important data, aiming to protect data included in the catalogues.

Therefore, although laws and regulations have defined “important data” and provided identification guidelines from a national level perspective, the catalogues of important data for each region and industry have not yet been issued, resulting in a certain degree of ambiguity as to how to define important data for enterprises in their

actual business operations. In this regard, Article 2 of ***the Regulations on Cross-Border Data Flow*** sets out clear guidelines -adopting the same approach as the criteria for determining whether an enterprise is a CIIO, i.e., whether certain data has been notified by local and sectoral authorities as important data. Enterprises only need to pay attention to whether the relevant departments and regions have informed or publicly announced whether the data processed by the enterprise is important data, which to a certain extent has reduced the compliance pressure on enterprises and alleviated the "difficulty" to identify important data. Therefore, we recommend that enterprises pay close attention to the catalogues and lists of "important data" that may be announced by the competent authorities from time to time, make periodic confirmation on compliance of its proposed data outbound transfer, maintain active and transparent communications with the competent authorities, and promptly adjust the strategy of outbound transfer of data, in order to avoid the potential compliance risk.

XVI. What are the Requirements for Outbound Transfer of Important Data?

Data processors who transfer data outside the Chinese mainland are required to apply for security assessments of outbound data transfers[11]. (For detailed content, please refer to "Part 1 Fundamentals: VIII. What is the Procedure of Outbound Cross-Border Data Transfer Security Assessment?")

Before submitting outbound data transfer security assessments of data processors shall submit the outbound data transfer risk self-assessments, focusing on the assessments in the areas including the types and sensitivities of the data to be outbound transferred, and the risks that the outbound transfers of data may bring to national security, public interests, and the lawful rights and interests of individuals or organizations[12]. (For detailed content, please refer to "Part 2 Practice: XXXI. How to Submit Outbound Cross-Border Data Transfer Risk Self-Assessment? ")

[11] See Article 4 of *the Assessment Measures*.
[12] See Article 5 of *the Assessment Measures*.

XVII. What are the Specific Contents of the Standard Contract for the Outbound Transfer of Personal Information?

According to Article 6 of ***the Measures for the Standard Contract***, the standard contract shall be concluded in strict compliance with the model formulated by the CAC. The personal information processors may agree on additional provisions with overseas recipients, provided that these provisions do not conflict with the standard contract.

According to the Annex to ***the Measures for the Standard Contract***, the contents of the current edition of the standard contract model mainly include:

1. Basic information of the personal information processor and the overseas recipient, including but not limited to the name, address, contact name/title, and contact information;
2. The purpose, manner, scale, type, transfer method, retention period, and location of the personal information transferred overseas;
3. The obligations of the personal information processor and the overseas recipient to protect personal information, as well as the technical and management measures taken to prevent possible security risks arising from the outbound cross-border transfer of personal information;
4. The impact of the personal information protection policies and regulations of the overseas recipient's country or region on the performance of the contract;
5. The rights of the personal information subject, as well as the ways and means to protect the rights of the personal information subject;
6. Remedies, termination of the contract, liability for breach of the contract dispute resolution, etc.

Since the outbound cross-border transfer of personal information is one of the scenarios of personal information processing activities, it must follow the basic requirements of personal information processing activities stipulated in ***the Personal Information Protection Law***. Some clauses within the standard contract also reflect the general principles of personal information processing activities under ***the Personal Information Protection Law***. In addition, the Standard Contract stipulates the obligations of the data exporter and the data importer, which can be supplemented and

refined by the two parties through annexes or contracts.

It should be noted that, according to Article 6 of ***the Measures for the Standard Contract***, the personal information processor can agree on other provisions with the overseas recipient, provided that theses provisions do not conflict with the standard contract. For cases where the contracting parties have signed relevant agreements on cross-border data transfer before signing the standard contract, if the provisions of the relevant agreements conflict with the standard contract, the standard contract shall prevail.

XVIII. What are the Specific Requirements for the Personal Information Protection Certification?

The personal information protection certification is voluntary rather than compulsory and encourages qualified personal information processors to voluntarily obtain personal information protection certification for the collection, storage, use, processing, transfer, provision, public disclosure, deletion, and cross-border data transfer. For the "voluntary certification", personal information processors involved in cross-border transfer of personal information choose to be certified or not to be certified on a purely voluntary basis sincethe certification of personal information protection and the filing of standard contracts are parallel compliance paths. Even if certification is chosen, it is also necessary to determine whether the situation requires a outbound data transfer security assessment. If so, the personal information processor shall file the cross-border data transfer security assessment submission.

According to ***the Certification Rules***, personal information protection certification is based on ***GB/T 35273-2020 Information Security Technology - Personal Information Security Specification***. For personal information processors conducting cross-border data processing activities, the requirements of ***the Certification Measures for Outbound Personal Information Transfer (Draft)*** and ***the Certification Specification V2.0*** shall also be complied with. In principle, the data processor shall conduct the personal information protection certification in accordance with the latest edition of the above standards and policies.

For personal information processors registered in (applicable to

organizations)/located in (applicable to individuals) the Guangdong-Hong Kong-Macao Greater Bay Area, i.e. personal information processors in Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Dongguan, Zhongshan, Jiangmen, Zhaoqing and Hong Kong Special Administrative Region that conduct cross-border personal information transfer, shall comply with ***the Practical Guidelines to Cybersecurity Standards - Requirements for Protection of Cross-Border Personal Information in Guangdong-Hong Kong-Macao Greater Bay Area (Draft)***. The Guide consists of six parts: scope, definition of terms, requirements for processing personal information, basic principles, requirements for protecting personal information subjects' rights and interests, and requirements for personal information security. While emphasizing the requirements of ***the Personal Information Protection Law***, the Guide also incorporates the relevant provisions of ***the Personal Data (Privacy) Regulations of Hong Kong***, such as the need to obtain the consent of the personal information subjects for using personal information for commercial marketing.

GB/T 35273-2020 Information Security Technology - Personal Information Security Specification stipulates the principles and security requirements that should be followed in carrying out personal information processing activities such as collection, storage, use, sharing, transfer, public disclosure, and deletion. These requirements are oulined from seven aspects, including: collection, storage and use of personal information, rights of personal information subjects, entrusting handling of personal information, sharing, transfer, public disclosure, disposal of personal information security incidents, and organizational personal information security management requirements.

In addition, for conducting cross-border processing activities of personal information, ***the Certification Requirements for Cross-Border Transfer (Draft)*** sets out basic requirements for personal information processors in six aspects, including: legally binding documents, organizational management, rules for cross-border processing of personal information, Personal Information Protection Impact Assessment, rights of the subject of personal information, and responsibilities and obligations of personal information processors as well as overseas recipients, including:

1. Personal information processor and overseas recipient shall sign the legally

binding and enforceable documents to ensure that the rights and interests of personal information subjects are fully protected;

2. The personal information processor and overseas recipient conducting cross-border processing of personal information are required to designate a person in charge of personal information protection and establish a personal information protection organization;

3. The personal information processor and the overseas recipient conducting cross-border processing of personal information shall set up and comply with the same rules on cross-border processing of personal information;

4. The personal information processor shall submit the Personal Information Protection Impact Assessment and issue the report;

5. The personal information processor and the overseas recipients shall respond to the relevant rights and interests of personal information subjects;

6. The personal information processor and overseas recipient shall fulfill the corresponding responsibilities and obligations.

Meanwhile, although ***the Certification Measures for Outbound Personal Information Transfer (Draft)*** does not explicitly list the list of specific materials that need to be submitted when a personal information processor applies for outbound personal information protection certification, the Certification Rules issued in 2022 stipulate that the certification entrustment materials should include, but are not limited to, the basic materials of the certification entrustee, the letter of attorney for certification, and relevant supporting documents. Meanwhile, according to the results of our consultation with the China cybersecurity review, certification and market regulation big data center(CCRC) as well as the “Answer to Reporter's Question on <the Regulations on Promoting and Regulating Cross-Border Data Flow>” issued by the CAC on March 22, 2024, enterprises can apply for certification through the certification management system for the protection of personal information (https://data.isccc.gov.cn) to the CCRC for application. Processors of personal information can refer to the Certification Rules and the Personal Information Protection Certification Application Form posted on the official websites of the CCRC to familiarize themselves with what certification materials they need to prepare.

The processor of personal information shall also prepare materials sufficient to demonstrate the compliance of the evaluated matters in accordance with the key evaluated contents of the outbound personal information protection certification as stipulated in the ***the Certification Measures for Outbound Personal Information Transfer (Draft)***, as follows:

(1) Legality, legitimacy, and necessity of the purpose, scope, and method of personal information exportation: The personal information processor is required to develop an argumentative explanation of the legality legitimacy, and necessity of the cross-border transmission of the matter. Legality requiresthat activities involving the outbound personal information transfer must have a legal basis, have the legitimacy of the subject of the personal information agreeing individually to the outbound data transfer activities, and are not prohibited by laws and regulations. Legitimacy requires that the purpose of the exit of personal information should be clear and reasonable; and necessity includes the necessity of the purpose and the scope of personal information (i.e., the purpose of the outbound has a direct relationship with the personal information that is exported, and the amount of personal information that is exported is minimized). (i.e., the purpose of departure is directly related to the outbound personal information and the quantity is minimized).

(2) Impact of the personal information protection policies and laws of the country or region of the overseas personal information processor and the overseas recipient and the network and data security environment on the security of outbound personal information: The personal information processor shall sort out the laws and regulations on personal information protection of the country or region of the overseas personal information processor and the recipient and whether the local law enforcement and judicial organizations are perfect, etc., in order to prove that the country/region of the overseas country/region's personal information protection policies and laws, and the network and data security environment are perfect. The personal information protection policies and laws of the overseas countries/regions and the network and data security environment will not have a negative impact on the security of outbound personal information.

(3) Whether the level of protection of personal information of overseas personal information processors and overseas recipients meets the requirements of the laws and

administrative regulations of the People's Republic of China and mandatory national standards: personal information processors may elaborate in this part whether the country/region is a member of international organizations related to data protection, whether it has made binding international commitments in respect of data protection, or whether it has concluded bilateral or multilateral agreements with China on data circulation and sharing, etc. (iii) Whether the country/region is a member of an international organization related to data protection, has made binding international commitments on data protection, or has concluded bilateral or multilateral agreements with China on the flow and sharing of data.

(4) Whether the legally binding agreement concluded between the processor of personal information and the overseas recipient has agreed on the obligation of personal information protection: If the processor of personal information and the overseas recipient have signed a data processing agreement (DPA), the DPA should set up special clauses agreeing on the responsibilities and obligations assumed by both parties in terms of personal information protection, so as to ensure the safety of the outbound data.

(5) Whether the organizational structure, management system and technical measures of the personal information processor and overseas recipient can adequately and effectively safeguard data security and the rights and interests of personal information: the personal information processor shall provide a specific explanation of whether it has set up a personal information protection department or management body, whether it has established a PIPO post, and what technical protection measures it has taken in respect of the cross-border activities of personal information, and so on.

Since the outbound PIPO certification and standard contract filing are applicable under the same circumstances, and there is a great overlap between the content of the assessment and the matters covered by the Personal Information Protection Impact Assessment Report, we believethat when submitting the outbound PIPO certification materials,a Personal Information Protection Impact Assessment can be submitted to the certificant institute as evidence of compliance

The above laws and regulations can not only serve as the relevant basis for

certification institute to implement the certification of cross-border processing activities of personal information, but also provide reference for personal information processors to standardize their cross-border processing activities of personal information.

XIX. What are the Penalties for Failing to Comply with the Outbound Data Transfer Regulations?

The Assessment Measures do not provide for additional responsibilities and penalties for non-compliance, but rather referring the relevant penalties under ***the Cybersecurity Law***, ***the Data Security Law,*** and ***the Personal Information Protection Law***. At the same time, if the data processor constitutes a crime, it will be held criminally liable in accordance with the law, specifically:

According to Article 66 of ***the Cybersecurity Law***, CIIOs who store network data outside the Chinese mainland, or provide network data outside the Chinese mainland in violations of regulations, the relevant competent departments shall order CIIOs to make corrections, give a warning, confiscate illegal gains, and impose a fine of no less than CNY50,000 but no more than CNY500,000. Additionally, the authorities may order CIIOs to suspend relevant business, suspend business for rectification, close down the website, or revoke the relevant business permits or licenses. For the persons directly in charge or other directly responsible personnel, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.

According to Article 46 of ***the Data Security Law***, relevant competent departments have the right to order those, who transfer important data outside the Chinese mainland in violation of regulations, to make corrections, give warnings, and impose a fine of no less than CNY100,000 but no more than CNY1,000,000.00. The persons directly in charge or other directly responsible personnel may be imposed a fine of no less than CNY10,000 but no more than CNY100,000. In case of serious scenarios, relevant competent departments have the right to impose a fine of no less than CNY1,000,000.00 but no more than CNY110,000,000.00, and order the data processors to suspend business, suspend operation for rectification, or revoke business permits or licenses. The persons directly in charge or other directly responsible personnel may face a fine

of no less than CNY100,000.00 but no more than CNY1,000,000.00.

According to Article 66 of ***the Personal Information Protection Law***, if the enterprise processes personal information in violation of regulations and fails to perform the relevant compliance processes, it may face severe penalties such as a fine of no more than CNY50 million or no more than five percent of the previous year's turnover. The enterprise may also face the penalties of the suspension of relevant businesses, suspend operation for rectification, or revoke relevant business permits or license. Meanwhile, the persons directly in charge or other directly responsible personnel may face a fine of no less than CNY 100,000.00 but no more than CNY 1,000,000.00 and may be prohibited from serving as directors, supervisors, senior managers, or the persons in charge of relevant enterprises within a specific period of time.

According to Article 253 of ***the Criminal Law of the People's Republic of China*** (***the Criminal Law***), those who violate relevant state regulations by selling or providing citizens' personal information to others, if serious, shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall be fined concurrently or exclusively. If the scenarios are especially serious, the offender shall be sentenced to fixed-term imprisonment of no less than three years but no more than seven years and shall also be fined. Those who, in violation of regulations, sell or provide citizens' personal information obtained in the course of performing duties or providing services to others shall be punished severely according to the provisions of the preceding paragraph. Those who steal or illegally obtain citizens' personal information by other means shall be punished according to the provisions of the first paragraph. If a unit commits a crime stipulated in the preceding three paragraphs, it shall be fined, and the person directly in charge and other person directly liable shall be punished according to the provisions of each paragraph.

XX. What other Specific Matters should be Noted?

According to ***the Law of the People's Republic of China*** on Guarding State Secrets, transferring state secrets abroad in violation of the law may constitute a crime and result in criminal liability.

In addition, the enterprise should also be aware of the criminal liability stipulated in ***the Criminal Law***, such as Article 111 of ***the Criminal Law***, which stipulates that whoever steals, spies into, buys, or unlawfully supplies state secrets or intelligence for an organ, organization or individual outside the territory of China shall be sentenced to fixed-term imprisonment of no less than five years but no more than 10 years. If the scenarios are especially serious, the offenders shall be sentenced to fixed-term imprisonment of no less than 10 years or life imprisonment; if the scenarios are minor, the offenders shall be sentenced to fixed-term imprisonment of no more than five years, criminal detention, public surveillance or deprivation of political rights.

If a particular field or industry is involved, the enterprise is also required to search the laws and regulations, departmental rules, and other normative documents to confirm whether there are any applicable special provisions in order to avoid being penalized.

XXI. Does China's Guangdong-Hong Kong-Macao Greater Bay Area Have Special Facilitation Measures for Outbound Cross-Border Transfer of Personal Information?

On June 29, 2023, the Hong Kong Innovation, Technology and Industry Bureau and the Cyberspace Administration of China signed ***the Memorandum of Cooperation on Promoting Cross-Border Data Flows in the Guangdong-Hong Kong-Macao Greater Bay Area*** (***the Cooperation Memorandum***) to reduce the risk of cross-border data flow and compliance costs, and promote the development of digital economy and scientific research in the GBA.

In order to implement ***the Memorandum of Cooperation***, the Hong Kong Innovation, Technology and Industry Bureau and the CAC jointly issued ***the Implementation Guidelines for the Standard Contract for Cross-Border Flow of Personal Information in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)*** on December 13, 2023 (***the Implementation Guidelines***). The Implementation Guidelines clarify that personal information processors and recipients in the GBA can follow the requirements of ***the Implementation Guidelines*** by concluding the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) Personal Information Cross-Border Flow Standard Contract between the

mainland and Hong Kong in the GBA (except for those information that has been notified by relevant departments and regions or publicly released as important personal information).

The GBA Standard Contract is applicable to personal information processors and recipients who are registered (applicable to organizations)/located (applicable to individuals) in nine mianland cities in the GBA (i.e. Guangzhou City, Shenzhen City, Zhuhai City, Foshan City, Huizhou City, Dongguan City, Zhongshan City, Jiangmen City and Zhaoqing City) and Hong Kong. The implementation rules are applicable to not only the cross-border flow of personal information from mainland cities in the GBA to Hong Kong, but also the cross-border flow of personal information from Hong Kong to the mainland cities in the GBA. They are not applicable to the cross-border flow of personal information between the Mainland and Macao.

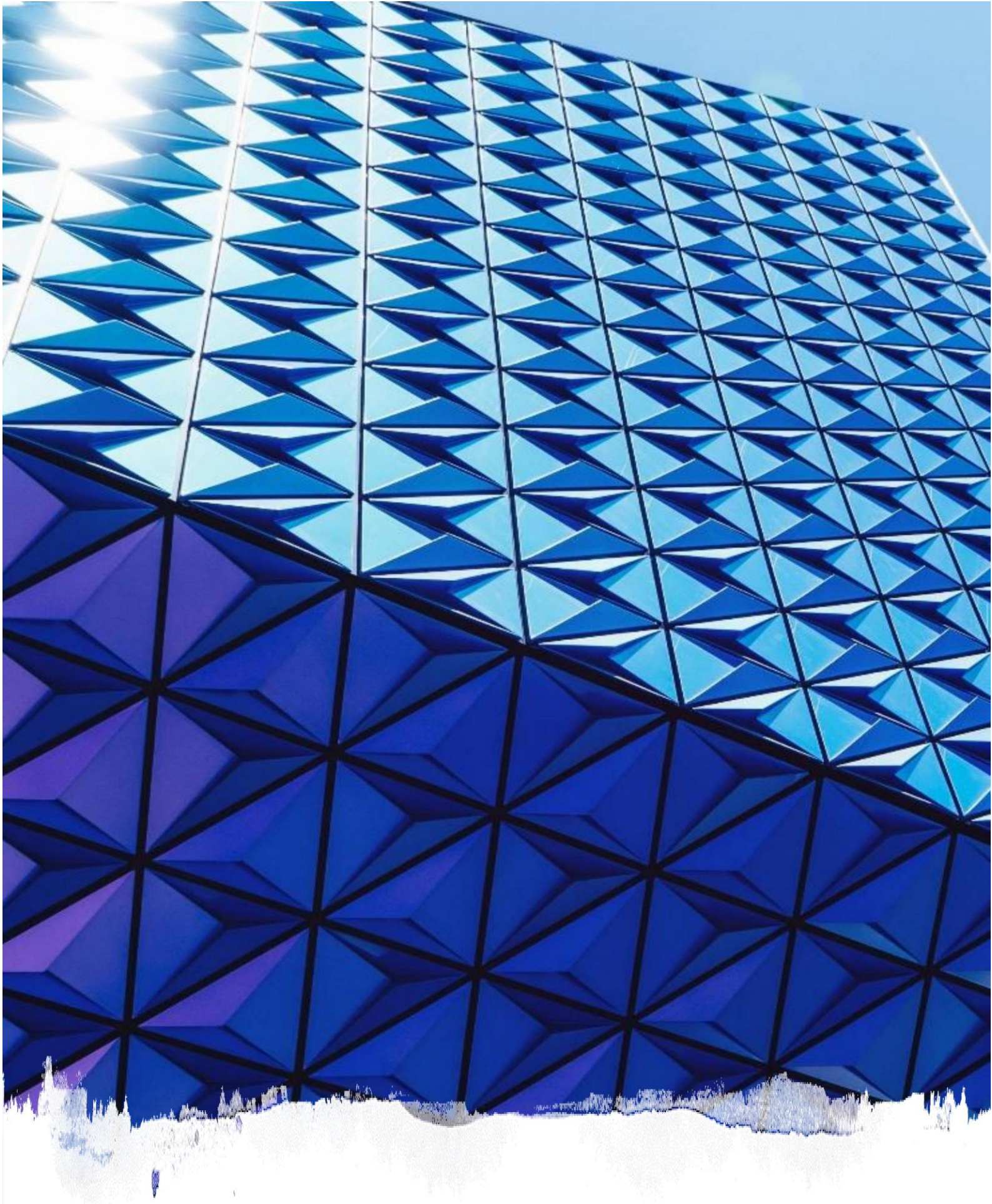
According to the Office of the Chief Information Officer of the Hong Kong SAR Government, ***the GBA Standard Contract*** is a measure designed to simplify the compliance arrangements for cross-border flow of personal information between the mainland and Hong Kong in the GBA. It is voluntary and allows individuals and institutions in both locations to enter into standard contracts based on a unified template to standardize the responsibilities and obligations of both parties to the contract in terms of personal information protection. Personal information that flows cross-border through ***the GBA Standard Contract*** shall not be provided to organizations or individuals outside the GBA.

It is worth noted that personal information processors and recipients who concluded ***the GBA Standard Contract*** shall make filing with the Cyberspace Administration of Guangdong Province or the Office of the Chief Information Officer of the Hong Kong SAR Government according to their jurisdiction within 10 working days from the date of the standard contract taking effect, and submit the photocopy of the ID of the legal representative, undertaking letter, and the standard contract.

Compared with the filing requirements for Chinese Mainland's standard contracts, although the filing requirements for ***the GBA Standard Contract*** are exempted from the obligation to submit a Personal Information Protection Impact Assessment Report, cmpanies are still required companies to independently submit the Personal Information Protection Impact Assessment work and make compliance commitment based on the

assessment results. Therefore, for personal information processors who have signed ***the GBA Standard Contract***, submitting Personal Information Protection Impact Assessment serves an effective tool to strengthen the enterprise's own risk management capabilities. ***The GBA Standard Contract*** simplifies the filing procedures. On one hand, it facilitates the cross-border flow of personal information of organizations and individuals in the GBA. On the other hand, it does not completely relax the requirements for submitting impact assessment of personal information protection for relevant organizations and individuals.

Therefore, enterprises in the GBA that engage in cross-border data flow activities can consider signing ***the GBA Standard Contract*** with relevant parties in the region to enhance the compliance of outbound activities on the premise of meeting the provisions of ***the Implementation Guidelines***. At the same time, enterprises should also pay attention to fulfilling relevant personal information protection compliance obligations to avoid hitting regulatory red lines.



PART 2 PRACTICE

XXII. How to Identify Scenarios of Cross-Border Data Transfer?

Based on ***the Guidelines to Assessment Submission (Second Edition)*** and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***, "data transfer" includes: (1) The data processor transfers data outside the Chinese mainland, the data were collected and generated in the course of the operating within the Chinese mainland; (2) The data processor stores the collected and generated data within the Chinese mainland, which can be accessed, retrieved, downloaded and exported by institutions, organizations or individuals outside the Chinese mainland; and (3) other data processing activities, such as processing personal information of natural persons outside the Chinese mainland. (For detailed content, please refer to "Part 1 Fundamentals: II. What Activities Constitute Cross-Border Data Transfer?")

Therefore, enterprises need to pay attention to the following points when determining whether the "data transfer" is involved:

1. Whether the data is collected and generated in the course of operating within the Chinese mainland;
2. Whether the enterprise's conduct is an act of providing data outside the Chinese mainland, or whether the relevant data can be "accessed, retrieved, downloaded, exported" from outside the Chinese mainland; and
3. Whether other data processing activities, such as the processing of personal information of natural persons within the Chinese mainland are in accordance with the Paragraph 2 of Article 3 of ***the Personal Information Protection Law***, that is, the activities of processing the personal information of natural persons either for: A. for the purpose of providing products or services to natural persons ; B. analyzing and evaluating the conduct of natural persons; or C. other scenarios specified in laws and administrative regulations.

1. Whether data is collected and generated in the course of the operating within the Chinese mainland

Before determining whether data is collected and generated in the course of the operating within the Chinese mainland, the meanings of "within the Chinese mainland" and "Operation" should be clarified.

There are two types of meaning of "within China": "within the territory of China" and "within the Chinese mainland". The former, "within the territory of China" refers to the territory over which the state exercises its sovereignty, including the mainland of China, the Hong Kong Special Administrative Region, Macao Special Administrative Region and Taiwan Region (hereinafter collectively referred to as Hong Kong, Macao and Taiwan Regions). The latter. "within the Chinese mainland" refers to the area where the same customs law or tariff system are applied[13]. According to the definition provided in ***the Exit and Entry Administration Law of the People's Republic of China***, "outbound transfer" refers to traveling from the Chinese mainland to other countries or regions, including traveling from the Chinese mainland to Hong Kong Special Administrative Region or Macao Special Administrative Region, and traveling from the Chinese mainland to Taiwan. Under this definition, Hong Kong, Macao and Taiwan Regions are "outside the Chinese mainland". Article 13 of ***the Network Security Management Regulations (Draft)*** specifies that "any data processor listing in Hong Kong which affects or may affect the national security" shall apply for network security review in accordance with relevant provisions. It can be concluded from the above that laws and regulations on cross-border data transfer also tend to interpret the term "within China" from the perspective of "within the Chinese mainland", that is, they deem the transfer of data from the Chinese mainland to Hong Kong, Macao and Taiwan Regions as an "outbound transfer".

As for "operating within the Chinese mainland", it is generally recognized within the industry that definition refers to the conduct of business and provision of products or services. In practice, if an enterprise only provides services outside the Chinese mainlandand does not collect data within the Chinese mainland, such activity will not deemed to be an "operating within the Chinese mainland". For example, if a network operator within the Chinese mainland conducts business and provides products or services for institutions, organizations or individuals outsidethe Chinese mainland, and are not involved in the processing of personal information and Important data within the Chinese mainland this will not be considered as an "the operating within the Chinese mainland".

[13] See *the Guidelines for Explanation and Application of Provisions of the Personal Information Protection Law*, edited by Prof. Zhou Hanhua, Institute of Law, Chinese Academy of Social Sciences, Beijing: Law Press, 2022, P244.

2. Whether the act falls into the three types of data transfer?

The act of data transfer involved in enterprise practice is generally divided into the three following types:

- **The data processor will transfer and store data outsidethe Chinese mainland that were collected and generated in the course of the operating within the Chinese mainland.**

In practice, the following are some scenarios in which may be identified as data transfer:

a) Transferring data outside the Chinese mainlandthrough various data delivery methods (Figure 6)

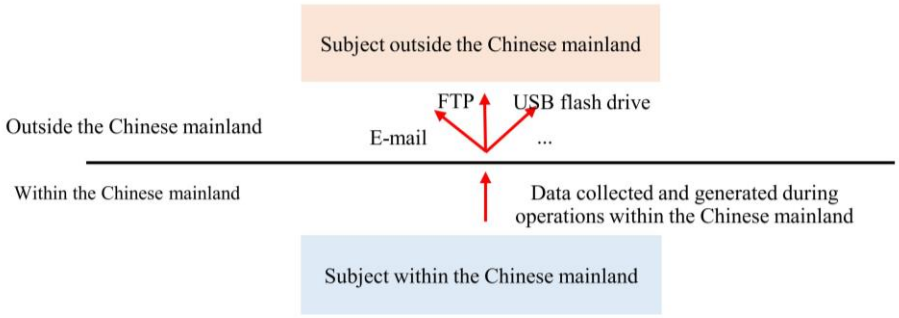


Figure 6

Software, hardware and other physical media with the function of data transfer may include e-mail, FTP, cross-border VPN, API or the common USB flash drive, mobile hard disk, mobile phone or portable notebook. This scenario is an easily identifiable scenario of data transfer.

b) Uploading or storing data to a server or cloud outside the Chinese mainland (Figure 7)

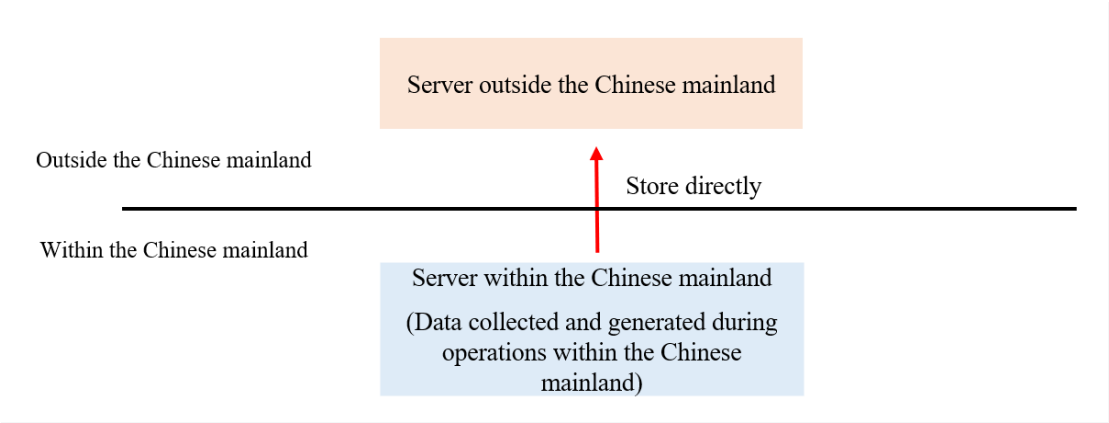


Figure 7

If an enterprise's information system, software platform or database server or cloud is deployed outside the Chinese mainland (for example, a multinational corporation uses an information system operated and/or deployed by a service provider outside the Chinese mainland), this will also be deemed as data transfer.

c) Transferring data outside the Chinese mainland through third parties (Figure 8)

In addition, the data transfer activity between subjects within and outside the Chinese mainland often involves a third party. For example, an enterprise located outside the Chinese mainland may entrusts a third party supplier within the Chinese mainland or outside the Chinese mainland to collect data generated from operations within the Chinese mainland on its behalf. In this scenario, although the data is not collected directly by the enterprise outsidethe Chinese mainland, it will still be deemed to be the data processor if the third party vendor is entrusted by it to process the data, and is therefore still likely to be considered to be a recipient located outside the Chinese mainland.

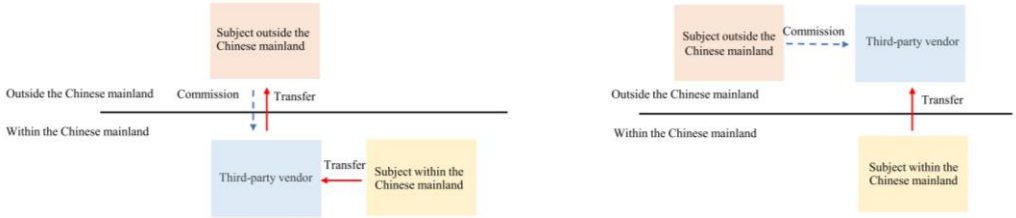


Figure 8

- **Where data collected and generated are stored within the Chinese mainland by a enterprise, and can be accessed, retrieved, downloaded and exported (except public information and website access) by enterprises. institutions, organizations or individuals outside the Chinese mainland, such activity will also be considered as data transfer.**

In determining data transfer activity, attention should also be paid to whether subjects outsidethe Chinese mainland can acquire/access data that is located within the Chinese mainland. That is to say, no matter how the data transfer is conducted between subjects within and outside the Chinese mainland, as long as the subject outsidethe Chinese mainland accesses, retrieves, downloads and exports the data generated in the course of operation within the Chinese mainland, it should be deemed as data transfer (Figure 9).

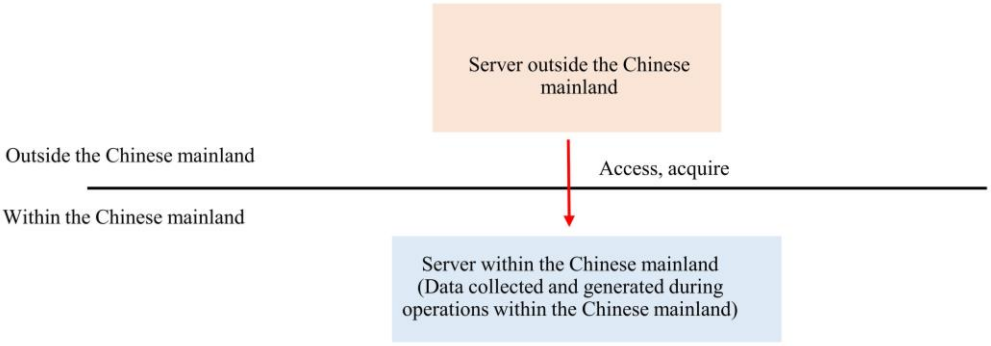


Figure 9

The accessing, retrieving, downloading, exporting of any data stored within the Chinese mainland by the transnational corporation, parent, subsidiary of the same economic/business entity will also considered as data transfer. For example, accessing by Foreign Invested Enterprise (FIE)'s overseas parent enterprise to data stored on FIE's servers in China is considered as data transfer.

- **Processing of personal information of natural persons within the Chinese mainland and other data processing activities outside the Chinese mainland**

Apart from the above two scenarios, ***the Guidelines to Assessment Submission (Second Edition)*** and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)*** cover a the third type of data transfer, "activities outside the Chinese

mainland to process personal information of natural persons and other personal information which falls under the scenarios specified in Article 3 (2) of ***the Personal Information Protection Law***".

Specifically, Article 3 (2) of ***the Personal Information Protection Law*** states, "This Law shall also apply to the activities outside the Chinese mainland to process the personal information of natural persons within the Chinese mainland if any of the following scenarios is involved: (1) The purpose is to provide products or services to natural persons within the Chinese mainland; (2) Analyzing and evaluating the activities of natural persons within the Chinese mainland; or (3) Other scenarios prescribed by laws and administrative regulations."

"For the purpose of providing products or services to natural persons within the Chinese mainland" can be interpreted as a cross-border transaction with the Chinese mainland as the target market and the individual as the transaction object. With regard to whether relevant personal information processors outside the Chinese mainlandtake the Chinese mainland as their target market, the commercial intentions of such processors will be judged by taking into account a variety of factors, for example, if the websites or applications of such processors outsidethe Chinese mainland use the Chinese language to mark or introduce relevant products and services; if RMB is used as payment currency or is connected to the payment instruments within the Chinese mainland, etc., may lead regulators to conclude a processor outsidethe Chinese mainland has the Chinese mainlandas their target market[14].

Regarding "analyzing and evaluating behavior of natural persons within the Chinese mainland", it is similar to the concept of "Monitoring of EU Customers' Behaviour" in ***the General Data Protection Regulation (EU) 2016/679*** *(hereinafter referred to as "**GDPR**")*[15]. GDPR Recital 24 states that "In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him

[14] See *the Interpretation of Personal Information Protection Law*, edited by Yang Heqing, Legislative Expert of the Economic Law Office of the Legislative Affairs Commission of the Standing Committee of the National People's Congress, Beijing: Law Press, 2022.
[15] See *the Understanding and Application of Personal Information Protection Law*, edited by Cheng Xiao, Beijing: China Legal Publishing House, 2021.

or for analyzing or predicting her or his personal preferences, behaviours and attitudes". Referring to the above concepts, "analyze and evaluate" can be interpreted as analyzing or predicting a person's behavior habits, hobbies or economic, health or credit status, through continuous recording and tracking of relevant personal information, and through follow-up processing technologies[16]. For example, a Chinese user browses the international website of a recruitment platform to view job information in an overseas job market and registers a user account. The headquarters of the platform in the United States analyzes and evaluates the personal information of the Chinese user, and based on this, sends a personalised push message about the job position to the Chinese user. Such activity will be considered as "analyzing and evaluating the conduct of natural persons within the Chinese mainland" by a processor located outsidethe Chinese mainland, and therefore constitutes data transfer.

"Other scenarios provided by laws and administrative regulations" is a catch-all provision. Considering that the development of new technologies and new applications may bring challenges to regulating personal information processing activities, the catch-all provision provides necessary flexibility for relevant laws and administrative regulations to deal with new issues arising from the administration of cross-border processing activities.

XXIII. What are Potential Cross-Border Data Transfer Scenarios that Enterprises May be Involved in?

1. Data Transfer Scenarios of Human Resource Management

◆ **Enterprise Recruitment (cross-border transfer of the candidates' personal information)**

For multinational enterprises, the following are typical scenarios that may involve the data transfer:

Enterprises with headquarters located outsidethe Chinese mainland may recruit employees via their official websites hosted outside the Chinese mainland. To apply for

[16] See the *Annotated Version of the Personal Information Protection Law of the People's Republic of China*, Law Press Law Press, 2022.

a job, candidates are invited to to fill in their personal information. (Figure 10).

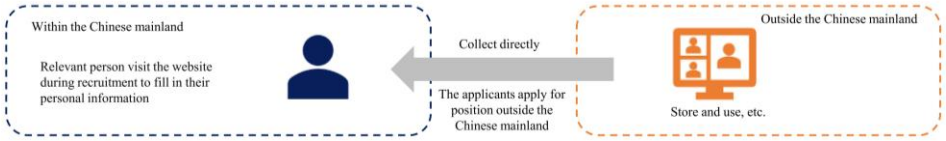


Figure 10

An enterprise within the Chinese mainlandmay upload a candidate's personal information collected within the Chinese mainland to a server within the Chinese mainland, and a foreign enterprise outsidethe Chinese mainland (eg. its parent enterprise) is given access and retrieve rights to the data on the server. (Figure 11)

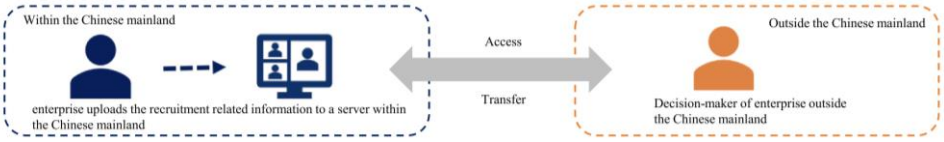


Figure 11

Enterprises within the Chinese mainland may hire a third-party vendor to collect information on candidates and transfer such data to an enterprise located outside the Chinese mainland. (Figure 12)

Figure 12

In addition, it is worth noting that, during recruitment, an enterprise will usually collect such personal information such as a candidate's name, gender, contact information, education background and work experience, etc. However, since the enterprise has yet to enter into an employment contract with the candidate, the provision in the Item 2, Paragraph 1 of Article 13 of ***the Personal Information Protection Law***, which refers to the scenarios necessary for implementing human resources management on the basis of the employment rules and regulations, cannot be taken as a legal basis

for the collection of personal information. Therefore, in this case, the legal basis for processing personal information must rely on "obtaining the individual's consent" under Item 1, Paragraph 1 of Article 13 of ***the Personal Information Protection Law***. To obtain consent, the candidate must first be informed of the purposes of processing their personal information, and their personal information must not be transferred abroad_a, until the explicit authorization by way of separate consent is obtained from the candidate in accordance with the law.

◆ **Data Transfer Scenarios of Employee Data**

Human resources management activities commonly include the following scenarios which involve the data transfer:

Regular transfer of employee data by HR and other relevant personnel to recipients outsidethe Chinese mainland by e-mail or in other means (Figure 13)

Figure 13

HR and other relevant personnel within the Chinese mainland may upload employee data to a HR system within the Chinese mainland that allows others outsidethe Chinese mainland to remotely access the data or where overseas employees visit the Chinese mainland to access such data (Figure 14).

Figure 14

Collection data of employee within the Chinese mainland by subjects outside the Chinese mainland through Global HR Management Systems (Figure 15)

Figure 15

◆ Data Transfer Scenarios of Business Data

There are mainly three scenarios of data transfer that may occur when carrying out business activities: Firstly, enterprises within the Chinese mainland may collect personal information of users through ToB and ToC business and transfer such information outside the Chinese mainland or allow others located outside the Chinese mainland to access the data stored within the Chinese mainland. Secondly, enterprises, at the request of their headquarters within the Chinese mainland, may directly store data generated during their operation (such as production, technology and business data, Important/Core data, etc.) in overseas servers, or store such data on servers within the Chinese mainland, but allow others outside the Chinese mainland to access, retrieve, download, export the above data stored on the servers within the Chinese mainland; Thirdly, enterprises located outside the Chinese mainland may directly collect the personal information of users within the Chinese mainland (Figure 16).

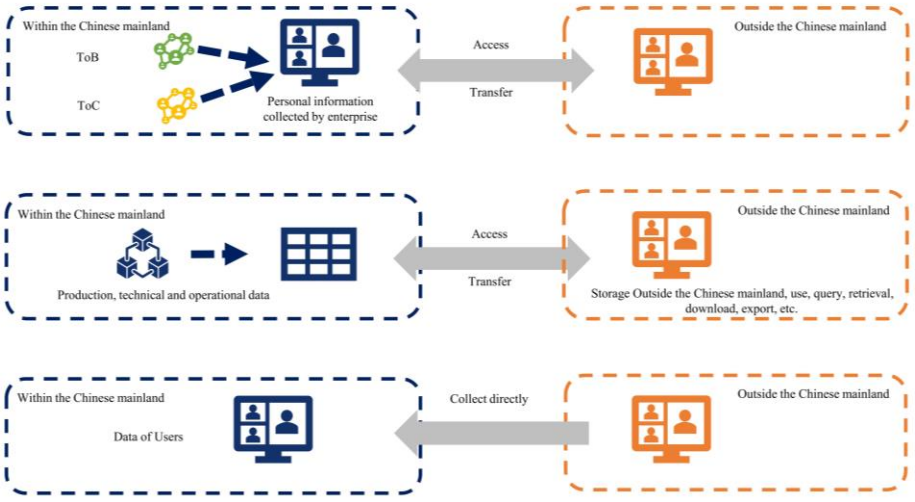


Figure 16

It is worth noting that in the above scenario, the enterprise may engage a third-party vendor and entrust it with data processing (e.g. engaging a salary management

vendor to process employees' personal information). In such a scenario, the enterprise remains the data processor/data provider for the data transfer, while the third-party vendor acts only as a entrusted processor or technology provider.

XXIV. How to Accurately Identify the Type of Cross-Border Data Transfer?

In practice, enterprises may often encounter challenges in identifying personal information, sensitive personal information and important data.

1. Identification of Personal Information

Both ***the Personal Information Protection Law*** and ***the Cybersecurity Law*** clarify the concept of personal information with the criterion of whether the information can be used to "identify" or "identifiable" as a natural person's personal identity. However, any information which has been anonymized is not personal information[17].

Enterprises who wish to conduct de-identification or anonymization of personal information should note that, although the personal information after anonymization is no longer personal information as the relevant individual cannot be identified, the personal information after de-identification is still personal information if the relevant individual can be identified again with the help of additional information. For example, if the enterprise had transferred to an overseas recipient complete fields of the user's mobile phone number, address, name, etc. and the overseas recipient retains these fields in its database. In this case, even if the outbound enterprise adopts de-identification measures in the current data transfer, the overseas recipient may still identify the information to a specific individual by means of database cross-referencing or user ID mapping. In this case, the data transferred abroad retains the attributes of personal information and should be considered as cross-border transfer of personal information.

2. Identification of Sensitive Personal Information

According to ***the Personal Information Protection Law***, sensitive personal information refers to personal information that, once disclosed or illegally used, is

[17] See Article 4 of *the Personal Information Protection Law*; and Article 76 of *the Cybersecurity Law.*

likely to infringe upon the dignity of a natural person or jeopardize the safety of a person or property, including information on biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts and movement, and personal information of minors under the age of 14[18]. Compared with personal information, the impact of damage to sensitive personal information will be more serious. Appendix B of ***GB/T 35273-2020 Information Security Technology - Personal Information Security Specification*** lists some types of sensitive personal information to provide enterprises with guidance for their compliance practices.

On whether de-identification can result in sensitive personal information being no longer sensitive, based on the consultation with regulatory authorities such as the Provincial Cyberspace Office, if de-identification processing can change the nature of sensitive personal information, personal information obtained after such processing will no longer be sensitive personal information. In other words, if sensitive personal information that has gone through the de-identification process is disclosed or illegally used, and neither the disclosure nor the illegal use will result in the damage to the dignity of the natural person or the endangerment to the personal or property safety of the natural person, then the sensitive personal information that has gone through the de-identification process will not be sensitive personal information.

3. Identification of Important Data

(For detailed content, please refer to "Part 1 Fundemantals: XV. What are the Legal and Regulatory Bases for Identifying Important Data?")

XXV. How to Account for the Quantity of Data Transferred Across Border?

When creating an inventory of the quantity of cross-border transfer data, enterprises may focus on the following points:

1. Quantifying the Amount of Data

Prior to the release and implementation of ***the Regulations on Cross-Border Data***

[18] See Article 28 of *the Personal Information Protection Law.*

Flow, the quantity of cross-border transfer data should be counted with full consideration of the relevant parties involved in the data processing process. For example, in addition to personal information of users collected by the enterprise, the information of employees within the enterprise and business contacts such as customers and suppliers are personal information to which the general rules on data transfer apply. Therefore, when counting the amount of personal information, especially when determining whether the threshold of Outbound Cross-Border Data Transfer Security Assessment has been reached, enterprises must count not only the number of C-end users, but also the number of internal employees and B-end contacts such as customers and suppliers.

However, according to Article 7, paragraph 2 and and Article 8, paragraph 2 of ***the Regulations on Cross-Border Data Flow*** and ***the Q&A on the Regulations on Promoting and Regulating Cross-Border Data Flow***, it can be inferred that before counting the number of cross-border data to determine whether it meets the threshold conditions for the submission of the outbound data transfer system, enterprises should assess whether they can rely on the exemptions put forward by ***the Regulations on Cross-Border Data Flow***, namely, (1) that the data transferred outside the Chinese mainland is data that is collected and generated in international trade, cross-border transportation, academic cooperation, transnational manufacturing, marketing and other activities and do not contain personal information and important data; (2) Personal information outside the Chinese mainland (not involving personal information or important data within the Chinese mainland) is processed in the country and its subsequent provision outside the Chinese mainland; (3) the data involves personal information that is transferred outside the Chinese mainland for the purpose of entering into or performing a contract to which the individual is a party; (4) the data involves personal information of employees and is transferred outside the Chinese mainland for the implementation of cross-border human resources management in accordance with labor rules and regulations and collective contracts signed in accordance with the law; (5) the data involves personal information which is provided outside the Chinese mainland for the emergencies; (6) where the data processor who is not a critical information infrastructure operator, has not transferred outside the Chinese mainland the personal information of less than 100,000 persons since January 1st of the current year and such data, does not contain sensitive personal information; (7) where the data

processor that is in a Free Trade Zone transfers data outside the Chinese mainland and such data is not in the Negative List for Pilot Free Trade Zone (FTZ negative list). Where the above exemptions apply, other than for item (6) above, the data processor will not not need to include such data when calculating the cumulative quantity of personal information that is transferred outside the Chinese mainland.

It should also be noted that ***the Q&A on the Regulations on Promoting and Regulating Cross-Border Data Flow*** and ***the Outbound Cross-Border Data Transfer Security Assessment Submission（Template）*** further clarifies that: (i) when counting the amount of data transfer of personal information, should be based on results with duplicates removed (measurement reference is the number of natural persons); and (ii) where there are a large number of recipients outside the Chinese mainland and the scope of the recipients is uncertain and it is not possible to enumerate them one by one, the statistical data can be provided at the time of the submission (more detailed explanatory notes on the actual operation of this requirement have yet to be provided by the regulator).

In addition, when counting the quantity of cross-border data, apart from scenarios where data is transferred from within the Chinese mainland to another country, data collected within the Chinese mainland during visits by others located outside the Chinese mainland should also be considered as cross-border data transfer (For detailed content, please refer to "Part 2 Practice: XXII. How to Identify Scenarios of Cross-Border Data Transfer? "), and the amount of data involved should also be counted in the total amount of cross-border data. For example, where employees from outside the Chinese mainland access domestic databases or foreign employees who visit China and access domestic databases, data accessed by such employees should also be counted as part of the total amount of data which has been assessed. The data processor may consider using network traffic monitoring methods to detect and record the mode of cross-border data, the destination IP of cross-border data, and identify the amount of data transferred outside the Chinese mainland or when others outside the Chinese mainland access data located within the Chinese mainland by using an IP address database. Based on our consultation with regulatory authorities, the amount of data where access is accessed by others outside the Chinese mainland should be calculated as the amount of data that is accessible by that parties that are outside the Chinese mainland.

2. The Relevant Time for Calculations

The Assessment Measures for Data Transfer and ***the Measures for the Standard Contract*** use "since January 1st of the current year" as the starting point for calculating the amount of data transferred outside the Chinese mainland, and count the cumulative amount of personal information/sensitive personal information provided by an enterprise outside the Chinese mainland since January 1st of the current year. After ***the implementation of the Regulations on Cross-Border Data Flow,*** the cumulative amount of cross-border transfer of personal information in the previous year is no longer used, and instead, calculations are now based on "January 1 of the current year" until the date of Outbound Cross-Border Data Transfer Security Assessment Submission. Although both statistical methods are based on the amount of cross-border data by enterprises in the past, the latter shortens the time period for calculating the amount of data transferred, and the threshold for the submission of the outbound data transfer system have been raised to a certain extent.

In addition, it should be noted that ***the Report on the Outbound Cross-Border Data Transfer Risk Self-Assessment (Template)*** also requires that data processor involving the cross-border transfer of personal information not only need to calculate and include the amount of data of natural persons transferred outside the Chinese mainland for the current year in their *Self-Assessment Report*, but must also estimate the amount of cross-border data for the next three years.

XXVI. How to Identify Internal Department Responsible for the Implementation of Compliance Measures for Cross-Border Data Transfer?

When an enterprise implements compliance measures for cross-border data transfer, it may require the cooperation of several departments such as legal affairs, information security and security operations and maintenance, audit and internal control, human resources.

Among them, where the enterprise does not have a data processing officer (DPO), the legal department is usually responsible for assisting the relevant departments in identifying the various types of data involved in the course of business, sorting out the

domestic and overseas transfer links of various types of data, and determining the data processing relationships and roles (e.g., entrusted processor or data processor) between the enterprise and other parties such as its partners and suppliers. The information security and security operation and maintenance department is usually responsible for sorting out data transfer security operation procedures and measures, establishing data security management system, formulating contingency plans for data transfer security incidents, and arranging relevant emergency response plans and drills. The audit and internal control department is usually responsible for auditing the adequacy and effectiveness of data export-related security policies, management systems, data transfer operation procedures and security measures formulated by the above departments. In addition, depending on the differences in data transfer scenarios, data transfer compliance work may also require the participation and cooperation of human resources departments or other business departments.

When considering which department should take the role of the lead department when conducting data cross-border transfer compliance work, enterprises should keep in mind that the lead department will need to formulate and implement effective compliance measures to address identified risks and coordinate and monitor the implementation of such measures with relevant departments, it should have sufficient professional capabilities and resources, including professional knowledge and comprehensive experience in legal, technical and risk management aspects. In practice, in the absence of a DPO, the legal department of an enterprise generally assumes the role of the lead department and engages a third-party consulting organization (e.g., a law firm, etc.) to provide assistance and advice to ensure that all aspects of data transfer are legally compliant.

XXVII. How to Determine the Submission of the Outbound Cross-Border Data Transfer Security Assessment?

According to Article 2 of ***the Assessment Measures for Data Transfer***, the applicant who should submit the data security assessment is the data processor that provides important data outside the Chinese mainland and/or personal information collected and generated in its operations within the Chinese mainland.

It is worth noting that, according to ***the Guidelines to Assessment Submission (Second Edition)*** and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***, if an overseas applicant that has not established an office or a branch within the Chinese mainland provides products or services to a natural person within the Chinese mainland, this may involve the processing of personal information of a natural person within the Chinese mainland and it may be legally required to submit a security assessment, it should also comply with the provisions of ***the Assessment Measures for Data Transfer***. In addition, as Article 53 of ***the Personal Information Protection Law*** states that, "an overseas processor of personal information that provides products or services to natural persons within the Chinese mainland or analyzes or evaluates the behavior of natural persons within the Chinese mainland shall set up a specialized agency or designate a representative within the Chinese mainland responsible for dealing with matters relating to the protection of personal information, and shall report the name of the relevant agency or name and contact information of the representative to the department that performs personal information protection duties." Therefore, where the data processor obtains important data and/or personal information directly from outside the Chinese mainland and meets the above submission requirements, the data processor should set up/appoint and submit a submission of the name and contact information of its designated agency or representative within the Chinese mainland.

In addition, it is a common practice for enterprises to commission a third-party supplier to process data on their behalf while assuming that the supplier can submit a Outbound Cross-Border Data Transfer Security Assessment on its behalf. However, this cannot be generalized - if the third-party supplier only processes data in accordance with the purpose and scope of data processing entrusted to it by the enterprise, the third-party supplier assumes the role of an "agent" rather than the data processor, and therefore cannot act as the submission subject of the Outbound Cross-Border Data Transfer Security Assessment.

XXVIII. How to Determine the Timing for Outbound Cross-Border Data Transfer Security Assessment?

Considering the diversity and volume of data to be retrieved, reviewed and submitted for Outbound Cross-Border Data Transfer Security Assessment and the complexity of the overall submission process, while taking into account its business operation deadlines, enterprises will need to ensure sufficient time for the data consolidation, material preparation and review, rectification and contracting stages when planning the timetable for Outbound Cross-Border Data Transfer Security Assessment Submission.

Many enterprises underestimate the time required for completing self-assessment and compliance rectification.Although it is called a self-assessment, in most cases, companies will hire external lawyers for the assessment, so adequate time should be allocated for this process. In the process of Outbound Cross-Border Data Transfer Security Assessment Submission, enterprises are often required to submit a series of materials, including Outbound Cross-Border Data Transfer Risk Self-Assessment Report, Outbound Cross-Border Data Transfer Security Assessment Submission, and Outbound Cross-Border Data Transfer related contracts or other legally binding documents with the overseas recipient[19]. In addition, Outbound Cross-Border Data Transfer Risk Self-Assessment work often involves the coordination and communication between multiple departments and should compliance gaps be identified, compliance rectification work must be carried out (e.g., improvement of the enterprise's internal system or revision of the signed *D*ata Processing Agreement, etc.). As enterprises need to spend a lot of time completing the Outbound Cross-Border Data Transfer Risk Self-Assessment work either by themselves or by commissioning third-party organizations, they should take account of their existing compliance status and start preparations early to avoid unwanted delays. It is important to note that the Outbound Cross-Border Data Transfer Risk Self-Assessment should be completed within 3 months of the date of submission of the outbound data security assessment submission[20]. Therefore, enterprises deploying Outbound Cross-Border Data Transfer security compliance work in advance should also pay attention to the completion date

[19] See Article 6 of *the Assessment Measures for Data Transfer*; Article 3 of *the Guidelines to Assessment Submission (Second Edition)* .
[20] See *the Outbound Cross-Border Data Transfer Risk Self-Assessment Report (Template),* Attachment 4 to *the Guidelines to Assessment Submission (Second Edition)*.

of the self-assessment activity before the submission. If the completion time of the self-assessment report is more than 3 months from the time of submitting the Outbound Cross-Border Data Transfer Security Assessment Submission, they should also resubmit the self-assessment and update the content of the report.

Second, enterprises should also reserve sufficient time for the review stage after the submission of materials. The overall length of the Outbound Cross-Border Data Transfer Security Assessment Submission is 57+N days (N represents the time for reviewing supplementary materials); if a reassessment is involved, it will be 72+N days (For detailed content, please refer to "Part 1 Fundemantals: VIII. What is the Procedure of Outbound Cross-Border Data Transfer Security Assessment?"). After submitting the submission, enterprises may need to modify, improve and supplement the submission materials several times according to the requirements of the National Internet Information Department. Since the laws and regulations do not limit the period for reviewing supplementary materials (i.e., N days out of the 57+N/72+N days mentioned above), the actual time required for the submission process may be much longer than 57 days or 72 days.

Therefore, enterprises should plan in advance, comprehensively consider the length of time they may take to submit self-assessment and compliance rectification work, and reserve time for the authorities to complete their review so as to avoid any negative impact to their business operations.

XXIX. Which Organization(s) Should the Enterprise Submit Outbound Cross-Border Data Transfer Security Assessment?

According to the provisions of ***the Guidelines to Assessment Submission (Second Edition)***, the data processor applying for online submission should submit materials through the data transfer submission system; while the data processor applying for offline submission should submit the Outbound Cross-Border Data Transfer Security Assessment to the National Internet Information Department through the provincial Cyberspace Administration Department where the data processor is located. (For detailed content, please refer to "Part 1 Fundemantals: VIII. What is the Procedure of Outbound Cross-Border Data Transfer Security Assessment?")

At the same time, we have set out in the form of an annex the submission channels for *Outbound Cross-Border Data Transfer Security Assessment* of national and provincial net information departments, so enterprises can consult and understand the relevant requirements for submission. (For detailed content, please refer to the "Annex I. The National and Provincial Cyberspace Administration Contact Information")

XXX. How to Submit a Personal Information Protection Impact Assessment?

Prior to cross-border data transfer, enterprises need to assess the security risks associated with data transfer based on their own business conditions and take appropriate measures to ensure their security. This is crucial for the legality and compliance of cross-border data transfer.

The first step of data transfer compliance procedures is to submit a Personal Information Protection Impact Assessment (hereinafter referred to as "PIA"), which is the self-assessment of the security risks associated with data transfer. According to Article 55 of ***the Personal Information Protection Law***, enterprises, as personal information processors, should submit PIA whenever there is a scenario of "transferring personal information outside the Chinese mainland". This requirement is also reiterated in Article 5 of ***the Measures for the Standard Contract***. In the meantime, Article 7 of ***the Measures for the Standard Contract*** provides that enterprises need to submit a PIA report if they use the Standard Contract for the Outbound Transfer of Personal Information as the compliant measures for the cross-border transfer of personal information. Annex 3 of ***the Guidelines to Recording Submission of Standard Contract (Second Edition)*** further requires that enterprises should complete the PIA report within three months prior to the date of record submission the standard contract, and that no material changes have occurred by the date.

Overall, enterprises should prepare PIA reports in accordance with Article 56 of ***the Personal Information Protection Law***, ***GB/T 39335-2020 Information Security Technology - Guidelines to Personal Information Security Impact Assessment***, ***the Measures for the Standard Contract***, and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)***. In particular, Annex 5 to ***the Guidelines to***

Recording Submission of Standard Contract (Second Edition), ***the Personal Information Protection Impact Assessment Report (Template)***, specifies that the PIA report used for record submission of standard contract for cross-border transfer of personal information should be prepared in strict accordance with the template, including the following details:

1. Overall situation of data transfer:

    - Basic information of the personal information processor, including introduction of the personal information processor, overall business and the processing of personal information, the situation of the personal information to be transferred outside the Chinese mainland and the situation of compliance with the relevant laws and regulations on the protection of personal information;
    - Basic information of the overseas recipient, including basic information of the overseas recipient, purposes and methods of processing personal information by the overseas recipient, and management and technical measures and capabilities of the overseas recipient to perform responsibilities and obligations;
    - Other scenarios that the personal information processor considers necessary to explain.

2. Details and conclusion of the impact assessment of activities to be transferred outside the Chinese mainland:

According to the following assessment items as specified in Article 5 of ***the Measures for the Standard Contract***, a provider should explain the results of the PIA, focusing on the problems identified by the assessment and the status of rectification, and draw objective impact assessment conclusions on the cross-border transfer of personal information with full explanations and arguments for the conclusions:

- Legality, legitimacy and necessity of the purposes, scopes and methods, etc., of processing personal information by the personal information processor and the overseas recipient;
- Scale, scope, types and sensitivity of the personal information to be

transferred outside the Chinese mainland, and the risks to personal information rights and interests arising from the outbound transfer of personal information;

- The obligations that the overseas recipient promises to undertake, and whether the management and technical measures and capacity for performing the obligations can guarantee the security of the personal information transferred outside the Chinese mainland; and
- Such risks as whether the personal information may be tampered with, destroyed, leaked, lost or illegally used after being transferred outside the Chinese mainland, and whether there is a unrestricted channel for data subjects to maintain their personal information rights and interests;
- The impacts of the personal information protection policies and regulations of the country or region where the overseas recipient is located on the performance of the standard contract;
- Other matters that may affect the security of cross-border personal information.

XXXI. How to Submit Outbound Cross-Border Data Transfer Risk Self-Assessment?

In addition to the PIA, when an enterprise meets any scenarios in which it is required to submit a Outbound Cross-Border Data Transfer Security Assessment Submission to the CAC, the enterprise should first submit a Outbound Cross-Border Data Transfer Risk Self-Assessment prior to making the submission. Although it is called self-assessment, enterprises usually recruit external lawyers to submit the assessment.

The Outbound Cross-Border Data Transfer Risk Self-Assessment Report (Template) which appears as Attachment 4 to ***the Guidelines to Assessment Submission (Second Edition)***, specifies that a self-assessment report shall be prepared in strict accordance with the template and include the following information:

1. Status of the self-assessment process;

2. Overall situation of data transfer:

- Basic information of the data processor, including introduction to basic information, organizational structure, information of the data security management institution, and overall business and data assets;
- Information of the data to be transferred outside the Chinese mainland, including:

  a) information of the business and data assets involved in the data to be transferred outside the Chinese mainland;

  b) purpose, scope, method, legality, legitimacy and necessity of the data to be transferred outside the Chinese mainland and the overseas recipient's processing of the data;

  c) information of sorting out corresponding data to be transferred outside the Chinese mainland based on business scenarios declared;

  d) information of the system platform and data center (including cloud services) for domestic storage of the data to be transferred outside the Chinese mainland;

  e) Information provided to other overseas recipients after the data has been transferred outside the Chinese mainland;

  f) information of the number of data to be transferred outside the Chinese mainland in the current year, and the number of data to be transferred outside the Chinese mainland in the next three years is estimated based on the statistics of natural persons (deduplicated);

- Information of the data processor's capabilities for safeguarding data security, including management and technical capabilities for safeguarding data security, proof of the effectiveness of data security safeguards, and compliance with relevant laws and regulations for data and network security;
- Information of the overseas recipient, including basic information of the overseas recipient, purposes and methods of data processing by the overseas recipient, and management and technical measures and

capabilities for the overseas recipient to perform its responsibilities and obligations;

- Information of responsibilities and obligations for data security protection agreed in legal documents, including:

  a) purpose, method and scope of data to be transferred outside the Chinese mainland, and purposes and methods of data processing by the overseas recipient;

  b) location and duration of storage of the data abroad, as well as measures to process the data to be transferred outside the Chinese mainland after the storage period has been met, the agreed purpose has been completed, or the legal documents have been terminated;

  c) restrictive requirements on the transfer of the data to be transferred outside the Chinese mainland by the overseas recipient to other organizations and individuals;

  d) security measures to be taken when the actual control or business scope of the overseas recipient changes substantially, or the data security protection policies or regulations or the network security environment of the country or region where the overseas recipient is located changes, or other force majeure events occur, making it difficult to ensure data security;

  e) remedies for breach of data security protection obligations agreed in legal documents, liability for breach of contract and dispute resolution methods;

  f) requirements to properly conduct emergency response when the data to be transferred outside the Chinese mainland is tampered with, destroyed, leaked, lost, transferred, illegally acquired or illegally used, and approaches and methods to protect individuals' personal information rights and interests;

- Other information that the data processor considers necessary to be explained.

3. Conditions and conclusion of the self-assessment of risks involved in outbound data transfer activities:

- Article 5 of ***the Assessment Measures for Data Transfer***, explains how self-assessment of risks should be submitted and focuses on the problems found in the self-assessment and the rectification thereof; and how to reach an objective conclusion on the self-assessment of risks by addressing:

  - The legality, legitimacy and necessity of the purpose, scope and methods of data transfer and processing the data by the overseas recipient;

  - The scale, scope, type and sensitivity of the data to be transferred outside the Chinese mainland, and the risks to national security, public interests and the legitimate rights and interests of individuals and organizations arising from the cross-border data;

  - The responsibilities and obligations promised by the overseas recipient, and whether the management and technical measures and capabilities for performing the responsibilities and obligations can guarantee the security of the data to be transferred outside the Chinese mainland;

  - Risks of the data to be tampered with, destroyed, leaked, lost, transferred, illegally acquired or illegally used during and after the data is transferred outside the Chinese mainland, and whether the channel for maintaining personal information rights and interests is smooth;

  - Whether the relevant data processing contracts to be concluded with overseas recipient or other legally binding documents have fully agreed on the responsibilities and obligations for data security protection;

  - Other matters that may affect the security of data to be transferred outside the Chinese mainland.

XXXII. Are PIAs and the Self-Assessment of Cross-Border Transfer Risks the Same in the Scenario of Cross-Border Data Tansfer?

It should be noted that a PIA is not the same as the Cross-Border Data Transfer Risk Self-Assessment. The PIA is a self-assessment that an enterprise is required to submit before the outbound transfer of personal information as expressly provided in Article 55 of ***the Personal Information Protection Law***, while the Outbound Cross-Border Data Transfer Risk Self-Assessment is a self-assessment that an enterprise is required by Article 5 of ***the Assessment Measures*** *for Data Transfer* to submit before outbound data transfers .

If the data transfer of personal information by an enterprise does not meet the reporting thresholds set forth in ***the Assessment Measures for Data Transfer*** and ***the Regulations on Cross-Border Data Flow***, the enterprise only needs to complete the PIA and be prepared to adopt relevant outbound data transfer systems (e.g. entering into and recording submission of standard contract or performing Personal Information Protection Certification) before it transfers the information outbound. However, if an enterprise meets certain conditions which require it to file for security assessment of outbound data transfer (For detailed content, please refer to "Part 1 Fundemantals: VII. Which Scenarios Fall under the Category of "Laws and Administrative Regulations Provide Otherwise, and Assessment/Approval Shall be Submitted in Accordance with Their Provisions"?"), in addition to submitting Outbound Cross-Border Data Transfer Risk Self-Assessment, the enterprise need to submit the PIA.

A comparison of the PIA assessment and Outbound Cross-Border Data Transfer Risk Self-Assessment reveals some similarities and differences.

PIA	Outbound Cross-Border Data Transfer Risk Self-Assessment
Article 56 of *the Personal Information Protection Law*: The assessment of impact on personal information protection shall include the following contents:	**Article 5 of *the Assessment Measures for Data Transfer*:** Prior to submit the Outbound Cross-Border Data Transfer Security Assessment, a data processor shall, in advance, submit a Outbound Cross-Border Data Transfer Risk Self-Assessment, and the self-

PIA	Outbound Cross-Border Data Transfer Risk Self-Assessment
(I) whether the purposes and means of personal information processing, are legitimate, justified and necessary; (II) the impact on individuals' rights and interests, and security risks; and (III) whether the protection measures taken are legitimate, effective, and compatible with the degree of risks	assessment shall focus on the following matters: (1) The legality, legitimacy and necessity of the purpose, scope and methods of the data transfer, and the processing of the data by the overseas recipient; (II) The scale, scope, type, and sensitivity of the data transfer, and the risks to national security, the public interest or to the legitimate rights and interests of individuals or organizations, caused by the data transfer; (III) The duties and obligations which the overseas recipient commits to perform, and whether the overseas recipient's organizational and technical measures and capabilities in terms of performing the duties and obligations can guarantee the security of the data transfer; (IV) The risks of the data being tampered with, destroyed, divulged, lost, transferred, illegally obtained or illegally used during and after the data transfer, and whether there is a smooth channel for safeguarding personal information rights and interests; (V) whether the responsibilities and obligations for data security protection are fully agreed in relevant contracts for the data transfer, or other legally binding documents to be concluded with the overseas recipient; (VI) Other matters that may affect the security of the data transfer.

From the perspective of concerns, PIA focuses on protecting the rights and interests of the subject of the personal information, including whether personal information processing is legitimate, justified and necessary, and whether security protection measures have been adopted. In terms of the Outbound Cross-Border Data

Transfer Risk Self-Assessment, emphasis is placed on the risks arising from data to be transferred outside the Chinese mainland to national security, public interests, and legitimate rights and interests of individuals and organizations.

In terms of content, the scope of the Outbound Cross-Border Data Transfer Risk Self-Assessment is larger than that of PIA. In addition to the content of PIA, the Outbound Cross-Border Data Transfer Risk Self-Assessment also includes determining whether the relevant data to be transferred outside the Chinese mainland contracts or other legally binding documents have fully stipulated the responsibilities and obligations for data security protection.

In general, under the scenario of cross-border transfer of personal information, although the focus of the Outbound Cross-Border Data Transfer Risk Self-Assessment is different from that of PIA, the objectives and basic content of the two are similar. Both require analysis and assessment of personal information to be transferred outside the Chinese mainland, screening out potential vulnerabilities and risks, and determining whether the adopted protection measures are sufficient to ensure the security of personal information.

In practice, PIA can often be combined with the Outbound Cross-Border Data Transfer Risk Self-Assessment. Enterprises do not need to submit two assessments and may submit a supplementary assessment on the basis of the content of PIA to fulfill the requirements of the Outbound Cross-Border Data Transfer Risk Self-Assessment. However, ***the Guidelines to Assessment Submission (Second Edition)*** requires that the Outbound Cross-Border Data Transfer Risk Self-Assessment Report should be prepared in strict accordance with the template. Therefore, when submitting a supplementary assessment on the content of PIA, enterprises should also ensure that the report is in full compliance with the template. In addition, the PIA report and processing record should be retained for at least three years. If an enterprise combines the PIA report with the report of Outbound Cross-Border Data Transfer Risk Self-Assessment, it should retain the report for at least three years.

XXXIII. How to Assess Whether the Technical and Organizational Measures of Data Processors and Overseas Recipient are Adequate?

According to Article 5 of ***the Assessment Measures for Data Transfer*** and ***the Outbound Cross-Border Data Transfer Risk Self-Assessment Report (Template)***, Appendix 4 of ***the Guidelines to Assessment Submission (Second Edition)***, before submitting a Outbound Cross-Border Data Transfer Security Assessment, the data processor shall submit a Outbound Cross-Border Data Transfer Risk Self-Assessment Report. In addition to assessing the processor's own ability to ensure the security of data to be transferred outside the Chinese mainland, the data processor should also assess "whether organizational and technical measures and capabilities in terms of performing the duties and obligations can guarantee the security of data transfer". Thus, proper assessment of the processor's ability to ensure data security is crucial for data to be transferred outside the Chinese mainland, and how to correctly and adequately assess the processor's ability to ensure data security is often a pain point for enterprises when submitting Outbound Cross-Border Data Transfer Risk Self-Assessment. We will elaborate on this by taking an assessment of the data processor's ability to ensure data security as an example.

The Outbound Cross-Border Data Transfer Risk Self-Assessment Report (Template), Appendix 4 of ***the Guidelines to Assessment Submission (Second Edition)***, lists the following criteria for assessing the data processor's ability to ensure data security:

1. Data security management capabilities, including management and organizational structures and construction of relevant systems, whole-process management, classification and grading, emergency response, risk assessment, protection of personal information rights and interests and the implementation of such systems (if cross-border transfer of personal information is involved, the enterprise shall provide to the CAC an additional description of its performance of Article 39 of ***the Personal Information Protection Law*** and evidence supporting such performance, including notification obligations and individual consents obtained from individuals, to the CAC. If the enterprise has legitimate grounds for the exemption of consent under ***the Personal Information Protection Law***, it is not required to obtain individual consents);

2. Data security technical capabilities, including technical security measures adopted throughout the process of data collection, storage, use, processing, transfer, provision, publication and deletion;

3. Certification of the effectiveness of data security measures, such as data security risk assessment, data security authentication, data security inspection and assessment, data security compliance auditing, and network security level protection evaluation, etc.;

4. Compliance with relevant laws and regulations on data and cybersecurity (if administrative penalties or regulatory corrections are required, additional evidence supporting the completion of corrections may be provided to the CAC).

Based on consultation with the regulatory authorities, we understand that the regulatory authorities will conduct a comprehensive review of the enterprise's relevant internal systems and the security technology in the process of data transfer when conducting their review of materials. In theory, all of the above should be reflected in the self-assessment report when covering the risks of the data transfer. The regulatory authorities will require sufficient details to be set out in the report so that they can correctly assess the enterprise's data security protection capability.

In practice, the assessment of an enterprise's data security protection capability is generally focused on two aspects: its management and organizational system support capability and its technical support capability:

1. Management system support capability

An enterprise shall, in accordance with relevant laws and regulations, describe in detail the management and organizational structures and systems construction relating to data security[21], such as internal systems for security management, personnel management, contractual constraints, audit mechanism, emergency response, protection of personal information rights and interests and the implementation thereof[22]. Generally speaking, the assessment of this part of security protection capability needs

[21] Relevant laws and regulations on data security protection include but are not limited to *the Data Security Law*, *the Network Security Management Regulations (Draft)*, *the Assessment Measures for Data Transfer* and *the Guidelines to Assessment Submission (Second Edition)*.

[22] See the Global Review | Outbound Data Transfer Compliance Guidance (II) — Submitting Outbound Cross-Border Data Transfer Security Assessment in accordance with Laws and Regulations — published by team of Maggie Meng, https://mp.weixin.qq.com/s/lFBeKQoEDx5bnL4lHGmCAQ.

to be completed by data compliance, legal, security, technical, audit and other departments through joint cooperation.

2. Technical means support capability

An enterprise shall have overall security protection technical means and a data security technical protection system to ensure the confidentiality, integrity and availability of the transferred data.

When submitting the assessment, enterprise should describe in detail such matters as the security measures taken, the ability to prevent, detect and respond to data security incidents, the ability to implement identity authentication and access control in the process of data transfer, the ability to retain data transfer log, and the ability to conduct audits of data transfer and end of life cycle measures[23]. As it is impossible to evaluate all aspects of the above technical means through simple written document review, it is recommended that enterprises consult technical experts in the relevant fields when submitting self-assessment, and submit a full assessment of the technical means support capability and obtain professional advice.

It should also be noted that enterprises are also required to provide proof of the effectiveness of data security protection measures, such as data security risk assessments, data security authentication, data security inspection assessments, data security compliance audits, network security level protection evaluation, ISO certification, etc.[24], so as to further support its position on its overall data security protection capability.

Based on our consultion with regulatory authorities, we understand that when assessing the data security capabilities of an overseas recipient, the criteria and standard by which an enterprise assesses the data security capabilities of the data processor shall be the same as that in which it assesses its own capabilities, regardless whether that data recipient is a local or overseas entity. The regulatory authorities has also indicated that the risk of data transfer will be assessed based on the data management system and data processing security measures of the overseas recipient when reviewing the report.

---

[23] Specific compliance obligations may be determined by referring to *the Assessment Measures for Data Transfer* and *the Guidelines to Assessment Submission (Second Edition)*.
[24] See *the Cross-Border Outbound Data Transfer Risk Self-Assessment Report (Template)*, Attachment 4 to *the Guidelines to Assessment Submission (Second Edition)*.

XXXIV. How to Assess the Adequacy of the Overseas Recipient's Legal and Policy Environment?

Although *the Outbound Cross-Border Data Transfer Risk Self-Assessment Report (Template)* and *the Personal Information Protection Impact Assessment Report (Template)* issued by the CAC provide that enterprises no longer need to assess the personal information protection policies and regulations of the overseas recipient's country or region when submitting the Outbound Cross-Border Data Transfer Risk Self-Assessment or PIA, this reduces the compliance burden on enterprises. It is important to note, however, that even if the enterprises are not required to state this in its Outbound Cross-Border Data Transfer Risk Self-Assessment Report or PIA Report. it is still recommended that enterprise still evaluate whether the personal information protection policies and regulations of the overseas recipient's country or region will affect its performance of its contractual obligations and document the evaluation process and results, as provided in Article 4 of ***the Measures for the Standard Contract*** issued by the CAC. Furthermore, Article 8 of ***the Assessment Measures for Data Transfer*** the CAC to consider "the impact of the data security protection policies and regulations as well as network security environment of the country or region where the overseas recipient is located, and the effect thereof on the security of cross-border data" when submit Outbound Cross-Border Data Transfer Security Assessment. This shows that the completeness of the overseas recipient's legal and policy environment is still a risk factor requiring attention. Enterprises are advised to first submit an assessment of the legal and policy environment of the overseas recipient's country or region before transferring any data abroad, so as to determine the potential security risks of the outbound data transfer.

According to ***the Assessment Measures for Data Transfer***, ***the Certification Specification V2.0***, ***the Guidelines for Security Assessment (Draft)*** and ***the Certification Requirements for Cross-Border Transfer (Draft)***, the following factors should be considered when assessing the completeness of the overseas recipient's legal and policy environment:

1. the impact of the data security protection policies and regulations as well as network security environment of the country or region where the overseas recipient is located, and the effect thereof on the security of the data to be

transferred outside the Chinese mainland;

2. whether the data protection level of the overseas recipient meets the requirements under the laws, regulations and mandatory national standards of the People's Republic of China;

3. the impact on the performance of the obligation to protect personal information and the protection of personal information rights and interests by the personal information protection policies and regulations of the overseas recipient's country or region, including:

    - previous experience of the overseas recipient with respect to cross-border processing of similar personal information, whether any data security-related incident occurred to the overseas recipient and was promptly and effectively dealt with by the overseas recipient; whether the overseas recipient has received any requests for personal information from public authorities in the overseas recipient's country or region and the overseas recipient has dealt with the requests;

    - the existing laws and regulations and generally applicable standards for personal information protection in the relevant country or region, and any differences with relevant laws, regulations and standards for personal information protection in the Chinese mainland;

    - regional or global organizations and binding international commitments made by the country or region in respect of personal information protection that the country or region joins;

    - the mechanism for personal information protection put in place in the country or region, such as whether there are supervision and law enforcement authorities and the relevant judicial authorities that are responsible for personal information protection.

4. Based on the legal and policy environment of the country or region where the overseas recipient of important data is located, the following factors may be assessed:

    - the existing laws, regulations and generally applicable standards on data security in the country or region;

- the law enforcement authorities and the relevant judicial authorities in charge of data security in the country or region;
- powers of the law enforcement authorities and the judicial authorities in the country or region to access relevant data and the relevant legal procedures therefor;
- whether the country or region has concluded bilateral or multilateral agreements on data flow and sharing with other countries or regions, including bilateral or multilateral agreements on data flow and sharing in respect of law enforcement, supervision, etc.

The legal and policy environment in the country or region where the recipient of personal information is located can be evaluated on a scale of "high, medium or low" by referring to the following criteria[25]:

High Level	Medium Level	Low Level
Laws and regulations governing the protection of personal information are relatively mature and systematic. Standards are widely used as a supplement to laws and regulations to protect various rights of subjects of personal information. There are special institutions for the protection of personal information, and meanwhile complete, effective and multi-level channels for remedies are in place.	The laws, regulations and standards governing personal information protection are basically complete to protect some rights of personal information subjects. There are relevant departments in charge of personal information protection and corresponding administrative and judicial channels for remedies.	The laws, regulations and standards governing personal information protection are deficient or incomplete, and individuals can only safeguard rights through judicial remedies.

The legal and policy environment of the country or region where the recipient of

[25] See Appendix B.3.3.1 to *the Guidelines for Security Assessment (Draft)*.

important data is located can be assessed on a scale of "high, medium or low", with reference to the following criteria[26]:

High Level	Medium Level	Low Level
The laws and regulations governing cyber security and data security are complete; the competent or regulatory authorities have strong supervision and enforcement capabilities, and effective accountability and supervision mechanisms after the occurrence of data security incidents. The power of law enforcement and judicial authorities to access relevant data is subject to laws, and the access is open and transparent, with no relevant negative cases reported recently.	The laws, regulations and standards governing cyber security and data security are basically complete, and the competent or regulatory framework takes initial shape. Data security incidents mainly rely on administrative supervision, and the access of data by law enforcement and judicial authorities to access relevant data shall be subject to certain procedures.	The laws, regulations and standards governing cyber security and data security are deficient or incomplete; the competent or regulatory authorities are not clear about or lack the corresponding capabilities; and there is no effective accountability mechanism after the occurrence of data security incidents. The power of law enforcement and judicial authorities to access relevant data is basically not subject to laws, or there have been relevant negative cases reported recently.

An a comprehensive and updated assessment of the legal and policy environment of the overseas recipient requires the assessor to have a full understanding of local policies, laws, culture, and society. We therefore recommend that enterprises shall remain in close contact with the overseas recipient, and it is recommended to engage lawyers or other multinational service organizations for assistance, so as to achieve a comprehensive and effective assessment.

[26] See Appendix B.3.3.2 to *the Guidelines for Security Assessment (Draft)*.

XXXV. What is the European Union's Approach to Assess Data Security Protection Policies and Legislation, as well as the Cybersecurity Environment?

As China has not yet provided explicit guidance on assessing the data security protection policies, legislation, and cybersecurity environment of countries or regions where overseas recipient is located, reference is made to the European Union's standards, which are recognized as leading practices in the field of data and privacy protection.

After the July 2020 Schrems II judgment of the Court of Justice of the European Union[27], to ensure that the overseas recipient will provide an essentially equivalent level of protection with those provided in the European Union, the European Data Protection Board (***EDPB***) adopted ***"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"*** and ***Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures*** [28]in November 2020, which provides guidance for submitting a Data Transfer Impact Assessment (**DTIA**) and highlight the importance of evaluating the legal frameworks and practices concerning personal data protection in third countries.

When assessing the legal environment of another country where an overseas recipient is located, EDPB explicitly requires adherence to four "European Essential Guarantees" and all relevant parties must comply with these guarantees to ensure a level of privacy and personal data protection that meets the standards required by the Court of Justice of the European Union and the European Court of Human Rights. When evaluating whether another country provides an essentially equivalent level of personal data protection to that of the European Union, it is crucial to evaluate whether the country's laws, particularly those pertaining to government access and the authority to require data disclosure, align with the European Essential Guarantees. These guarantees include:

---

[27] In this case, the Court of Justice of the European Union declared the Privacy Shield framework which provides for the possibility of lawful transfer of personal data from the EU to the United States invalid, on the ground that the overseas recipient (i.e., the United States) does not provide for an essentially equivalent level of personal data protection as the EU.

[28] （Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0）。EDPB updated and adopted *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 in June 2021*.

1. Data processing should be based on clear, precise and accessible rules: In addition to assessing whether there is a legitimate legal basis for processing personal data in the country or region where an overseas recipient is located, evaluation must also be made regarding the clarity, consistency, and enforceability of the legislation concerning personal data protection.

2. Limitations on the rights to privacy and to data protection must be necessary and proportionate to legitimate objectives and necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: It is emphasized that any limitations on personal rights and freedoms imposed by the legislation and administrative authorities of that country for the purpose of safeguarding national or public security must be justified in terms of necessity and proportionality.

3. An independent oversight mechanism should exist.

4. Effective remedies need to be available to the individual, including but not limited to, enforcement of rights of data subjects and right to seek remedies from judicial or other authorities when his/her rights are infringed.

On July 10, 2023, the European Commission adopted a adequacy decision for the EU-U.S. Data Privacy Framework[29]. The decision recognizes that U.S. companies participating in the EU-U.S. Data Privacy Framework can provide a level of data protection comparable to that of the EU. Under the new adequacy decision, personal data can transfer securely from the EU to U.S. companies certified under the EU-U.S. Data Privacy Framework without the need to implement additional data protection safeguards or further authorization.

Based on the applicable laws and regulations of China and European Union, when assessing the data security protection policies, legislation, and cybersecurity environment of the country or region where an overseas recipient is located, the following factors should be emphasized:

1. Legislation framework: The assessment should consider the applicable laws, regulations and standards concerning personal data protection, cyber security or data security in the country or region where the overseas recipient is located.

[29] https://www.dataprivacyframework.gov/EU-US-Framework.

It should also evaluate the differences between this legal framework and that of China;

2. International commitments: It is important to consider whether the country or region where the overseas recipient is located has joined any regional or global data protection agreements or has made any binding international commitments.

3. Enforcement mechanisms: The assessment should examine the enforcement mechanisms in the country or region where the overseas recipient is located, particularly in terms of personal data, cybersecurity, and data security. This includes evaluating whether there is a specified administrative authority and judicial authority responsible for data protection and the independence of such authorities. Additionally, it is important to determine whether there are effective accountability and supervision mechanisms in place to process data security incidents.

4. Powers of authorities: The assessment should examine the powers and legal procedures of the administrative and judicial authorities in the country or region where the overseas recipient is located. Key considerations include[30]:

    - Whether these powers are effectively restricted and subject to oversight.
    - Whether the execution of powers is conducted openly and transparently.
    - Whether there have been any recent cases that reflect negatively on this aspect.
    - Whether the overseas recipient has been required by local authorities to provide personal data.
    - How the overseas recipient has responded to such requirements.

5. Remedies available to data subjects: The assessment should examine whether the rights of data subjects are protected in the country or region where the

[30] See Section e)1), Article 5.4 of *the Certification Specification V2.0*.

overseas recipient is located. It should also consider whether there is a designated institution responsible for protecting personal data and whether a comprehensive, effective, and multi-tiered system of remedies is provided to data subjects.

6. International agreements: The assessment should examine whether the country or region where the overseas recipient is located has entered into any bilateral or multilateral agreements concerning data transfer or sharing. This includes agreements that pertain to enforcement or supervision mechanisms.

7. The assessment should also examine whether the country or region where the overseas recipient is located has adopted any prohibitive, restrictive or other similar measures in terms of data protection that are discriminatory in nature against China[31].

XXXVI. For How Long will a Outbound Cross-Border Data Transfer Security Assessment Result Remain Valid? Under What Scenarios is it Necessary to Resubmit for a Security Assessment?

Article 9 of ***the Regulations on Cross-Border Data Flow*** extends the validity period of the Outbound Cross-Border Data Transfer Security Assessment result from two (2) years to three (3) years, effective from the date when the assessment result is issued. In addition, ***the Regulations on Cross-Border Data Flow*** allows the data processor to apply for extension of the validity period of the security assessment results. If the data transfer activities are to be continued and there are no scenarios requiring a new submission of the security assessment, the data processor may apply for an extension of the validity period of its security assessment result. This submission should be made to the national cyberspace administration via the provincial-level cyberspace administration at the data processor's location, within sixty (60) working days before the expiration of the current validity period. Upon approval of the CAC, the validity period of its security assessment result may be extended for another three (3) years.

In addition, Article 14 of ***the Assessment Measures for Data Transfer*** stipulates

[31] See Kaiming CAI, Donghui Ruan, Brief analysis of *the Guidelines to Submission for Security Assessment of Outbound Data Transfers (Frist Edition)*, September 2022.

that the data processor must resubmitting the Outbound Cross-Border Data Transfer Security Assessment if any of the following scenarios occur during the validity term:

1. the new submission of Outbound Cross-Border Data Transfer Security Assessment is required if there is any change to the purpose, method, or scope of the data transfer, or if there is any change to the type of data, or change to the purpose or method of the data processing by the overseas recipient, which will affect the security of the data being transferred outside the Chinese mainland. Additionally, if the period for retaining personal information or important data is to be extended, a new submission is also required;
2. the new submission of Outbound Cross-Border Data Transfer Security Assessment is required if there is any change in the data security protection policies, legislation, or cybersecurity environment, or if any other force majeure event that has occurred in the country or region where the overseas recipient is located, or if there is any change in the actual control of the data processor or the overseas recipient, or if there is any change to the legal document executed between the data processor and the overseas recipient, which will affect the security of the data being transferred outside the Chinese mainland; or
3. the new submission of Outbound Cross-Border Data Transfer Security Assessment is required if there is any other scenarios that may affect the security of the data being transferred outside the Chinese mainland.

XXXVII. Under What Scenarios is it Necessary to Re-Conclude the Standard Contract and Record Submission for Cross-Border Transfer of Personal Information?

Article 8 of ***the Measures for the Standard Contract*** and ***the Guidelines to Recording Submission of Standard Contract (Second Edition)*** stipulate when the standard contract shall be supplemented or re-signed and re-recorded submission, they include:

1. When there is a change in the purpose, scope, type, sensitivity, method, or

storage location of the personal information transferred outside the Chinese mainland, or the method of processing personal information by the overseas recipient, or when the retention period of the personal information transferred outside the Chinese mainland is extended.

2. When there is a change in the personal information protection policies and regulations of the country or region where the overseas recipient is located that may affect the rights and interests of the personal information subjects;

3. Other scenarios that may affect the rights and interests of personal information subjects.

It is worth noting that when the above scenarios occur in addition to supplementing or re-concluding the standard contract and recording submission, the personal information processor must also re-submit the Personal Information Protection Impact Assessment and issue a report.

XXXVIII. Is it Possible to Modify the Standard Contract issued by the Regulatory Authority?

Article 6 of ***the Measures for the Standard Contract*** clearly stipulates that "the standard contract shall be concluded in strict compliance with the model formulated by the CAC, however the personal information processor can agree on other terms with overseas recipient as long as such terms are not in conflict with the standard contract."

Enterprise can supplement detailed information based on its actual situation regarding the cross-border of personal information in the annex to the standard contract. Annex II of the standard contract titled "Other Provisions Agreed by the Parties", allows the parties to agree on other provisions provided that they are not in conflict with the standard contract.

However, the enterprise should note that since these new provisions must not conflict with the standard contract, the new provisions only act as "supplementary provisions" (e.g., making specific agreements on the details of the management and technical measures to be adopted by the overseas recipient, etc.). Attention should be paid to ensure that the new provisions do not substantively adjust the terms of the

standard contract (e.g., by reducing the rights and interests of personal information subjects or reduce the responsibilities and obligations of the personal information processor/overseas recipient, etc.).

We have also listed the contact information of the National and Provincial CAC in the annex for your convenience. (For detailed content, please refer to "Annex I. The National and Provincial Cyberspace Administration Contact Information")

XXXIX. If a Data Processing Agreement with an Overseas Recipient already Exists, is it Permissible to Include a Standard Contract as an Attachment?

If an enterprise options to submit and record submission of standard contract as a compliance path for cross-border transfer of personal information, it must honor the obligations under the standard contract, even if a separate *Data Processing Agreement* has been concluded with the overseas recipient. It must conclude a standard contract in the same form as required by the CAC with the overseas recipient and record a submission of it through cross-border data transfer record system. The enterprise can include the standard contract as an attachment to a *Data Processing Agreement* with the overseas recipient.

If there is any doubt about the form, the enterprise can also refer to "Annex I. The National and Provincial Cyberspace Administration Contact Information" to confirm with the relevant cyberspace administration on any requirements based on their own specific situation.

XL. To whom should the Application of Personal Information Protection Certification be Submitted?

The Certification Announcement stipulates that certification bodies engaged in Personal Information Protection Certification must conduct relevant certification activities only after obtaining approval. However, there is no current list of qualified certification bodies under applicable laws and regulations.

CCRC issued an announcement [32], "CCRC is responsible for the specific implementation of Personal Information Protection Certification" on its official website. CCRC also published a template submission letter regarding Personal Information Protection Certification on its website and launched a "*Data Security Certification Management System*" (https://data.isccc.gov.cn) which covers the submission of Personal Information Protection Certification.

According to the consultations with CCRC and ***the Q&A on the Regulations on Promoting and Regulating Cross-Border Data Flow*** published by the CAC on March 22, 2024, for the purpose of outbound transfer of personal information, submission for *Personal Information Protection Certification* can be made to CCRC through the "*Personal Information Protection Certification Management System*" in the "Data Security Certification Management System" (https://data.isccc.gov.cn).

According to the Regulations of the People's Republic of China on Certification and Accreditation and the relevant provisions of ***the Certification Measures for Outbound Personal Information Transfer (Draft)***, professional organizations working in the field of data security and personal information protection need to meet the following requirements:

(1) Legally established: the organization needs to be established in accordance with the law, with independent legal personality, and must be approved by the State Market Supervision and Administration Department, obtain the qualification of personal information protection certification, and according to the law to the State Internet Information Department for the record of the certification body. (At the same time, since Article 8 of ***the Certification Measures for Outbound Personal Information Transfer (Draft)*** requires certification bodies to submit "professional work in the field of data security and personal information protection in the past three years" as the material for the record of the organization, we understand that this is equivalent to the establishment of an invisible threshold, i.e., the certification body is required to be an organization established for more than three years.)

(2) Professional capacity: professional and technical capacity related to the field of certification, and the capacity to accurately assess and certify data security and

[32] https://www.isccc.gov.cn/zxyw/sjaq/grxxbhrz/index.shtml, last accessed on March 23, 2024.

personal information protection. Capacity to formulate guidelines and procedures for carrying out outbound personal protection certification based on current and valid regulations and standards. Capacity to implement technical validation to effectively assess the security technologies and measures of personal information processors. This includes verification of technical architecture, data encryption, access control, etc. to ensure the security of personal information during the outbound process.

(3) Personnel requirements: a certain number of professional and technical personnel and managers who have the appropriate professional knowledge and practical experience to be able to assess the compliance of the organization's personal information processing activities and the effectiveness of its risk control measures.

(4) Management system: establish a sound internal management system and quality assurance system, including the formulation of detailed certification processes, certification implementation rules, work plans, audit standards and quality control measures to ensure the professionalism and standardization of the certification work. At the same time, there are dispute acceptance mechanisms and complaint handling mechanisms.

(5) Data security risk prevention: establish a data security risk prevention mechanism to ensure that the data in the certification process is free from the risks of tampering, destruction, leakage, loss, transfer or illegal access, illegal use and so on.

(6) Ongoing supervision: Establishing a post-certification supervision system to continuously supervise whether the exit activities of personal information conducted by certified personal information processors comply with the certification standards.

(7) Impartiality: the organization in carrying out certification activities, maintain independence and objectivity, to avoid conflicts of interest, should follow the principle of objectivity and impartiality, free from outside interference, to ensure that the authenticity and effectiveness of the certification results.

(8) information disclosure: open to the public the basis for certification, certification procedures, fees and other information, and accept social supervision.

XLI. How should Cross-Border Data Transfer be Properly Managed in the Context of International Dispute Resolution?

When involved in an international dispute, it is very common that one party will be required by an overseas judicial body to provide evidence materials that contain data or personal information stored in China. Under such scenarios, the issue of cross-border data transfer will be triggered.

Pursuant to Article 36 of ***the Data Security Law*** and Article 41 of ***the Personal Information Protection Law***, before providing any data or any personal information stored within the Chinese mainland to any foreign judicial or law enforcement body, approval of the competent China authorities must be obtained. The Ministry of Justice of the PRC clarified in *its Answers to Frequently Asked Questions on International Judicial Assistance in Civil and Commercial Matters* dated June 24, 2022, organizations or individuals within the Chinese mainland are prohibited from providing any data or any personal information stored within the Chinese mainland to any foreign judicial or law enforcement body without the approval of the competent China authorities.

Requests to provide any data or any personal information stored within the Chinese mainland to any foreign judicial or law enforcement body should be processed by the competent China authorities in accordance with applicable laws, treaties and agreements that China has concluded or acceded to, or in line with the principles of equality and reciprocity. In the context of international criminal matters, the National Supervisory Commission, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of National Security and other relevant departments serve as the competent authorities for international judicial assistance in criminal matters. Judicial assistance involving international criminal matters are handed by those authorities in accordance with ***the Law of the People's Republic of China on International Judicial Assistance in Criminal Matters*** and other applicable laws, as well as relevant international treaties and agreements. In the context of international civil and commercial matters, the Ministry of Justice of the PRC serves as the competent authority for international judicial assistance in civil and commercial matters. Judicial assistance involving international civil and commercial matters are managed by the Ministry of Justice of the PRC in accordance with *the Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in*

Civil or Commercial Matters, *the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, and the current 86 bilateral treaties on judicial assistance between China and other countries. If the judicial approach is not applicable, the Ministry of Foreign Affairs of the PRC will use a diplomatic approach instead.

However, recently it has become common in practice that when China entities are involved in civil dispute resolution processes outside the Chinese mainland, foreign courts or other judicial bodies require these entities to provide data and information stored within the Chinese mainland as evidence directly, rather than through the judicial or diplomatic channels. According to the responses provided by the Judicial Assistance Exchange Center of the Ministry of Justice of the PRC, the submission must be made to the Center, whether the evidence is requested by overseas judicial bodies, or submitted voluntarily by China entities. The submission procedure is as follows:

1. Submission letter, which should provide information such as a general introduction to the cases in which foreign courts are involved, and requests from such foreign courts regard evidence submission;

2. A list of evidence, which should provide a detailed explanation regrding the evidence materials intended for submission. This should include the name of each piece of evidence, the matters it is intended to prove, its relevance to the case, and whether it involves any information related to national security, state secrets, official documents, trade secrets, or personal information;

3. A self-assessment report, *i.e.*, the preliminary evaluation made by the entity concerning the evidence materials intended for submission;

4. A legal assessment report, *i.e.*, the legal opinion provided by legal department of the entity or an external law firm concerning the evidence materials intended for submission.

It is important to note that both the self-assessment report and the legal assessment report must clearly specify that the evidence materials intended for submission do not include any state secrets, that information invloving trade secrets has been redacted, and that individuals' separate consents have been obatined for contents involving personal information.)

After receiving the submission documents listed above, the Judicial Assistance Exchange Center of the Ministry of Justice, in conjunction with the Supreme People's Court of the PRC, the CAC, and the relevant industrial administrative authority of the entity (e.g., the Ministry of Industry and Information Technology of the PRC), will review the evidence materials intended for submission. In general, the time limit for the review will be 1-2 months; however, for significant or complex cases, the time limit will be extended to 2-4 months. If the review is passed, an approval will be issued to the applicant and the relevant material can then be provided overseas accordingly. Therefore, when facing the above scenarios, it it important to actively communicate with the Ministry of Justice to understand the procedures and documents required, and to prepare and submit their submission accordingly. The purpose is to avoide any possible delay in evidence submission that may be caused by an improper estimate of the time needed by the Ministry of Justice for its review and other unexpected issues that may arise during the review. Since the enactment of ***the Personal Information Protection Law*** and ***the Data Security Law***, many entities have made such submission to the Ministry of Justice and have obtained approvals.

With the enhancement of data security protection in China, the authorities involved have been making efforts make submission more convenient and improve the efficiency of the review process. For example, the overseas data transfer within the context of judicial procedures will be determined by the Ministry of Justice, which will be responsible for coordinating with other relevant authorities to review and approve the materials submitted by the applicant. The applicant may not be required to make a separate submission to the CAC. This approach can help the applicant save costs and improve the efficiency of where evidence needs to be transferred outside the Chinese mainland, as compared to having to make separate submission to the CAC and its industrial administrative authorities. In practice, we would suggest a timely review of the specific case to determine the reviewing authority, and early communication with such authority to confirm the required submission documents, procedures, and the time needed. This will be helpful for making overall arrangements in accordance with new administrative requirements.

XLII. How to Sign and Record the Submission of China's GBA Standard Contract for Cross-Border Transfer of Personal Information?

The GBA Standard Contract is a contract to be signed by personal information processor and receipients who are registered (for organizations) or located (for individuals) in the mainland part of GBA, or the Hong Kong Special Administrative Region when conducting cross-border personal information transfer activities. Personal information processor refers to those (in the case of the Mainland) organizations and individuals who independently decide the purpose and method of processing during processing activities, and (in the case of the Hong Kong Special Administrative Region) a "data user", which refers to, in terms of personal information, an individual who controls the data alone or jointly with other persons. Receiptient refers to organization or individual who receives personal information cross-border from the personal information processor. The main content of *the GBA Standard* Contract includes contractual obligations and responsibilities of both parties, rights of personal information subjects and related remedies, as well as contract termination, liability for breach of contract, dispute resolution etc.

Before personal information processors provide personal information across borders by entering into ***the GBA Standard Contract***, they should submit a Personal Information Protection Impact Assessment, focusing on the following:

(1) The legality, legitimacy and necessity of the purposes and methods of processing personal information by the personal information processor and the recipient;

(2) Impact on the rights and interests of personal information subjects and security risks;

(3) Whether the obligations promised by the recipient, as well as the management and technical measures and capabilities to perform the obligations, can ensure the security of personal information provided cross-border.

The personal information processor can agree on other terms with the recipient, but they must not conflict with ***the GBA Standard Contract***. If the purpose, scope, type, or method of cross-border provision of personal information, or the purpose or method of processing personal information by the recipient changes, the retention period is extended, or other scenarios occur that affect or may affect the rights and interests of

personal information, the personal information processor shall submit an impact assessment on personal information protection again, supplement or enter into the standard contracts again, and record submission procedures.

After ***the GBA Standard Contract*** is concluded and becomes effective, personal information processors and recipients can conduct personal information cross-border activities. Within 10 working days from the effective date of the contract, the personal information processor and recipient shall record submission with the Cyberspace Administration of Guangdong Province and the Office of the Government Chief Information Officer respectively according to their jurisdiction, and record submission of the required documents. In practice, the Cyberspace Administration of Guangdong Province does not directly accept record submission materials. Personal information processors and recipients should first record the electronic version of the submission materials (formal scanned PDF version and WORD version in CD) to the municipal level Cyberspace Administration. After the materials are reviewed for the completion, the the municipal level Cyberspace Administration will send them to the Cyberspace Administration of Guangdong Province for pre-examination. After the electronic version of the material is pre-examined, the personal information processor and recipient will deliver the hardcopies of the material (completely bound) and the attached electronic version of the material (in CD) to the Cyberspace Administration of Guangdong Province. The electronic version of the material should be consistent with the hardcopies in PDF scanned copy and WORD version. The Cyberspace Administration of Guangdong Province will process the materials after receiving them in accordance with the recording submission process.

The recording submission process of the GBA Standard Contract includes document submission, document inspection and reply to the recording submission results, supplementary or rerecording, etc. The recording submission documents include: a photocopy of the legal representative's identity document, a letter of commitment, and a signed version of the GBA Standard Contract. The Personal Information Protection Impact Assessment must be completed within 3 months before the recording submission date of the GBA Standard Contract, and no major changes have occurred as of the recording submission date. Compared with the recording submission requirements of the mainland's standard contracts, the Personal Information Protection Impact Assessment Report does not need to be submitted for recording.

The Cyberspace Administration of Guangdong Province will complete the material inspection within 10 working days after receiving the hard copy materials, and notify the personal information processor of the recording submission results. The recording submission results are either a pass or a fail. If the recording submission is passed, the Cyberspace Administration of Guangdong Province will issue a recording submission number to the personal information processor; if the recording submission is not passed, the personal information processor will receive a notification of unsuccessful recording submission and the reasons. If required to supplement the materials, the personal information processor should supplement the materials and rerecord submission within 10 working days.

If the purpose, scope, type, or method of cross-border of personal information, or the purpose or method of processing personal information by the recipient changes, the retention period is extended, or other scenarios occur that affect or may affect the rights and interests of personal information, the personal information processor shall re-submit a Personal Information Protection Impact Assessment, supplement or re-enter the GBA Standard Contract, and rerecord submission.

If the personal information processor supplements the GBA Standard Contract within the validity period of the GBA Standard Contract, it shall submit supplementary materials; if it re-enters the GBA Standard Contract, it shall make recording submission again. The inspection time for supplementary or rerecording submission is 10 working days.

XLIII. Are There any Regulatory Measures to Facilitate the Outbound Personal Information Transfer in the Shanghai Pilot Free Trade Zone?

Based on the provisions of Article 6 of ***the Regulations on Cross-Border Data Flow***, the pilot free trade zones are allowed to independently enact a negative list of data to which data transfer procedures applies. For any cross-border transfer data not under the negative list, the data transfer procedures will be exempted.

There are regulatory measures to facilitate the data transfer in Shanghai Pilot Free Trade Zone, which are mainly based on ***Shanghai Municipal's Implementation Plan of the Overall Program for Comprehensively Connecting with International High-***

standard Economic and Trade Rules and Promoting High-level Institutional Liberalization of China (Shanghai) Pilot Free Trade Zone *(Hu Fu Fa [2024] No. 1, effective on February 3, 2024, "the Implementation Plan")* and ***the Measures for Classification and Grading of Cross-Border Data Flow in Lingang Special Area of China (Shanghai) Pilot Free Trade Zone (for Trial Implementation)*** *(Hu Zi Mao Lin Guan Gui Fan [2024] No. 3, February 8, 2024, "the Lingang Measures").*

As mentioned above, ***the Regulations on Cross-Border Data Flow*** sets out a negative list mode in FTZs: under the national system framework of data classification and grading protection, develop a list of data ("the Negative List") in the FTZ that need to be included in the scope of Outbound Cross-Border Data Transfer Security Assessment, the Standard Contract for the Outbound Transfer of Personal Information, Personal Information Protection Certification. The Negative List shall be reported to the provincial-level cyberspace affairs commission for approval and then recorded submission to the national cyberspace administration authority and national data management authority for recording submission. Data transfer not under the Negative List by the data processor in the FTZs are exempted from submitting Outbound Cross-Border Data Transfer Security Assessment, concluding the Standard Contract for the Outbound Transfer of Personal Information, or passing the Personal Information Protection Certification(collectively, the "Data Transfer Procedures").

The Implementation Plan proposes that the Shanghai Pilot Free Trade Zone Administration and the Lingang Special Area Administration take the lead in formulating an important data catalog in accordance with the data classification and grading protection system and the actual needs of the zone; and proposes to establish a cross-border data service center in the Lingang Special Area to facilitate the data processor's self-assessment and other compliance activities for data transfer.

The Lingang Measures applies to the data processor, such as enterprise, public institution, association of institution and organization, which are registered within the Lingang Special Area or conduct activities related to cross-border data flow in the Lingang Special Area. In conjunction with the development of Shanghai's Five Centers and focusing on key fields such as automotive, finance, shipping, biomedicine and the development requirements of the relevant industries in the Lingang Special Area, ***the Lingang Measures*** encompass typical scenarios with the most urgent cross-border

needs as an entry point to classify and manage cross-border data transfer. ***The Lingang Measures*** categorize cross-border data into three grades and refine the regulatory requirements for outbound transfer of such data:

(1) Core Data refers to important data that have a high degree of coverage of a field, group, or region, or that reach a high degree of precision, a large scale, or a certain depth, which, once illegally used or shared, may have a direct impact on political security. Core data mainly includes data related to key fields of national security, data related to the lifeblood of the national economy, important people's livelihoods and major public interests, and other data that have been evaluated and determined by relevant state authorities. Core data is prohibited from being transferred outside the Chinese mainland.

(2)Important Data refers to data in a specific field, a specific group, a specific region, or data that has reached certain precision and scale, which, once leaked or tampered with or destroyed, may directly endanger national security, economic operation, social stability, public health and safety (data that affects only the organization itself or individual citizens is generally not regarded as important data). The data processor may apply for security assessment for cross-border data transfer through the cross-border data service center in Lingang Special Area regarding data within the important data list.

(3)General Data refers to data other than core data and important data. The data processor may apply for registration and recording submission with the Lingang Special Area Administration regarding data within the general data list and may freely transfer general data under the fulfillment of relevant management requirements.

The above mentioned important data catalog and the list of data included Data Transfer Procedures, etc. will be enacted by the Lingang Special Area Administration and will be submitted to the relevant authorities for approval and recording, and further updated and published. According to the Q&A of the press conference organized by the Information Office of Shanghai Municipal with the participation of various authorities, the general data list and the important data catalog of Lingang Special Area will be prepared and promulgated in accordance with the principle of "from enterprise to industry, from cases to lists, from positive aspects to negative aspects" in the short future, and will first focus on the key fields of intelligent connected vehicle, financing,

and high-end shipping.

The pilot general data lists of Lingang Special Area on the fields of intelligent connected vehicle, public offering of fund and biomedicine were promulgated by the Lingang Special Area Administration on May 16, 2024. According to the Lingang Special Area Administration, the negative list and other data lists is expected to be enacted subsequently. Also, according to relevant sources, we understand that there were precedents in practice where cross-border data transfer activities of enterprises registered in the Lingang Special Area can be recognized as being carried out in the Lingang Special Area and be subject to relevant exemptions, once such enterprises access the "Data Customs" through relevant data links in the Lingang Special Area. The data transfer can be conducted after taking certain archiving arrangement.

XLIV. Are There any Special Regulations for the Data Transfer in the Banking and Finance Industry?

In addition to general provisions mentioned in this ***Practical Q&A*****,** data compliance in banking and finance industry is also governed by relevant regulations promulgated by institutions such as the People's Bank of China. Those related to data transfer mainly include *the Personal Financial Information Protection Technical Specification (JR/T 0171-2020, implemented on February 13, 2020), the Financial Data Security—Guidelines for Data Security Classification (JR/T 0197-2020, implemented on September 23, 2020), and the Financial Data Security—Security Specification of Data Life Cycle (JR/T 0223-2021, implemented on April 8, 2021)*, etc.

For the identification and compliance requirements of critical information infrastructure operators in banking and finance industry. (For detailed content, please refer to "Part 2 Practice: XLV. Are There any Special Regulations for the Outbound Transfer of Data in Securities and Fund Industry?").

Regarding important data in banking and finance industry, ***the Financial Data Security—Guidelines for Data Security Classification*** sets out objectives, principles and scope of financial data security classification, as well as the elements, rules and classification process of data security classification. According to the impact object and the degree of impact caused by the damage of data security of financial institutions, the

data security levels can be categorized in descending order as Level 5, Level 4, Level 3, Level 2 and Level 1 . The characteristics of Level 5 data include (1) important data, which is usually used for key businesses of large or extra-large institutions in the financial industry, and institutions as important core nodes in the process of financial transactions; and generally, is available only to specific personnel and accessed or used only by those who need to know; and (2) where the data security is damaged, national security will be impacted or public interests will be seriously impacted.

Appendix C of the above Guidelines also specifies the identification of important data in banking and finance industry, specifically: (1) macro characteristics: data that can reflect economic and social characteristics that cannot be changed or remain stable over a long period of time; (2) derived characteristic data obtained from the aggregation of massive information: real transaction information of financial consumers covering multiple provinces after aggregation; (3) data in the decision-making and law enforcement process of industry regulators: controlled data collected and generated by administrative and law enforcement authorities in the course of performing their duties or enforcing the law that do not involve state secrets and are not disclosed; and (4) information on cybersecurity defects of critical information infrastructure: relevant vulnerability information on loopholes related to network equipment, servers, information systems, etc.

It shall be noted that important data mentioned above generally do not include enterprise production and operation, and internal management information, personal information, etc. *Financial Data Security—Security Specification of Data Life Cycle* mentions that the security classification and data protection of data collected and generated by branches, subsidiaries and other affiliates outside the Chinese mainland of banking and financial institutions in the course of their business operations outside the Chinese mainland shall be implemented in accordance with the requirements relating to cross-border data transfer. The Security Specification also emphasizes that financial data generated within the Chinese mainland should, in principle, be stored within the Chinese mainland, except as otherwise provided by the state and industry authorities. In particular, the Level 5 data generated within the Chinese mainland (including important data of the banking and finance industry) must be stored only within the Chinese mainland.

Nevertheless, according to ***the Regulations on Cross-Border Data Flow***, the data processor is not required to apply for security assessment for cross-border data transfer if such data has not been notified or published as important data by competent authorities or in certain areas. However, banking and finance institutions are still required to classify the data based on the foregoing provisions, and to adopt a more prudent attitude in cross-border data transfer that may involve important data.

Personal information is generally embodied in banking and finance industry as personal financial information. The definition of personal financial information in *the Personal Financial Information Protection Technical Specification* includes account information, identification information, financial transaction information, personal identification information, property information, debit and credit information and other information reflecting certain scenarios of the particular personal financial information subjects; and personal information is graded into three levels in this Technical Specification. Regarding the cross-border of personal financial information, personal financial information collected and generated in the course of providing financial products or services within the Chinese mainland shall be stored, processed and analyzed within the Chinese mainland. If it is necessary to provide personal financial information to institutions outside the Chinese mainland (including the head office, parent enterprise or branches, subsidiaries and other affiliates necessary for the completion of the business) due to business needs, the following requirements shall be fulfilled:

(1) it shall comply with the national laws and regulations as well as relevant provisions of the competent authorities of the industry;

(2) it shall obtain the explicit consent of the personal financial information subjects;

(3) it shall submit Outbound Cross-Border Data Transfer Security Assessment of Personal Financial Information in accordance with the methods and standards enacted by the state and the industry authorities concerned; and ensure that the data security protection capability of institutions outside the Chinese mainland meets the security requirements of the state, relevant industry authorities and financial institutions;

(4) it shall clarify and supervise institutions outside the Chinese mainland to effectively fulfill their duties and obligations in respect of confidentiality of personal

financial information, data deletion, and cooperation in investigation of cases, etc., through entering into agreements with institutions outside the Chinese mainland, on-site audit and other means.

The provisions of Appendix B of *the* ***GB/T 35273-2020 Information Security Technology - Personal Information Security Specification*** specify the sensitive personal information in banking and finance industry. In this Specification, sensitive personal information includes bank accounts, authentication information (code), deposit information (including the amount of funds, payment and receipt records, etc.), real estate information, credit records, credit investigation information, transaction and consumption records, bank statement records, etc., as well as information on virtual property such as virtual currencies, virtual transactions, and game redemption codes etc.

Banking and financial institutions should also pay attention to the relevant provisions of ***the Measures for the Administration of the Credit Reporting Business*** when transfer personal credit information outside the Chinese mainland. If banking and financial institutions meet relevant applicable conditions to constitute credit reporting entities, and provide entities outside the Chinese mainland with personal credit information, they should conduct necessary examinations of the identity of information users outside the Chinese mainland and the usage of the information to ensure that the information is used for reasonable purposes, such as cross-border trade, investment and financing, without endangering national security.

The Measures for Data Security Management in the Business Sector of the People's Bank of China (Draft for Comment) promulgated by the People's Bank of China also contains requirements on restrictions management of data transfer. Banking and financial institutions shall implement with reference to the Measures when it is formally promulgated and comes into effect.

XLV. Are There any Special Regulations for the Outbound Transfer of Data in Securities and Fund Industry?

In addition to general provisions mentioned in ***the Practical Q&A***, data compliance in securities and fund industry shall also pay attention to the relevant regulations promulgated by institutions such as the China Securities Regulatory

Commission (CSRC). Those related to cross-border data transfer mainly include *the Data Classification Guidelines for Securities and Futures Industry (JR/T 0158-2018, implemented on September 27, 2018), the Guidance for Data Security Management and Protection of Securities and Futures Industry (JR/T 0250-2022, implemented on November 14, 2022),* and *the Data Security Risk Prevention and Control for Securities and Futures Industry — Guidelines on Data Classification (GB/T 42775-2023, implemented on August 6, 2023)*, etc.

With respect to CIIOs, securities and fund industry institutions are generally considered to be CIIOs due to their connection with national economic and financial security, but as of the date of this Practical Q&A, no relevant lists of CIIOs issued or explicitly designated by the competent authorities of the securities and fund industry has been found through public channels.

With respect to important data of the securities and fund industry, ***the Data Classification Guidelines for Securities and Futures Industry*** was promulgated at an early stage and do not clearly specify what is important data, which results in some uncertainties in the connection with the current regulations on important data and the cross-border data transfer. The Guidelines aforementioned classify the data of the securities and fund industry into four levels based on impact objects (industry, institutions, clients), the scope of impact (multiple industries, multiple institutions within the industry, the institution itself), and the degree of impact (serious, medium, slight, none) incurred by the damage to the data security attributes (integrity, confidentiality, availability), and set out the requirements on the processing specifications of the securities and fund industry data: Level 4 (very high), the data is mainly used for the key business of large or extra-large institutions in the industry, and is generally available only to specific personnel and accessed or used only by those who need to know; Level 3 (high), the data is used for key business, and is generally available only to specific personnel and accessed or used only by those who need to know; Level 2 (medium), the data is used for general business, and is generally available to restricted subjects, and generally refers to internal management data and is not suitable for disclosure to the public; Level 1 (low), data can generally be disclosed or can be accessed and used by the public.

In the cross-border data activities of the securities and fund industry, it is also

worth noting that the classification changes due to data aggregation or prescription as mentioned in the Guidelines. Specifically, in the process of data transfer, delivery and use, due to various business needs, it may be necessary to aggregate data of the same or different levels for analysis and processing. For such data aggregation, it should be noted that: (1) when data from different channels or systems aggregate together for business needs, the original use of the data or the system where it is stored will change, and such data needs to be re-classified and re-graded; (2) in order to accurately determine the exact level, it needs to conduct in-depth analysis of whether the aggregated data may obtain more information than the original data, and to determine the impact after the damage of the data security nature (integrity, confidentiality, availability); (3) the level of aggregated data shall generally not be lower than the highest level of the original data aggregated. Similarly, attention should also be paid to the impact of data prescription on data classification and grading. We believe that the above principles are possible to be applied in the identification of important data and the compliance on the cross-border data transfer in the securities and fund industry.

Data Security Risk Prevention and Control for Securities and Futures Industry — Guidelines on Data Classification basically adopts the provisions on grading in the Data Classification Guidelines for Securities and Futures Industry; ***the Guideline for Data Security Management and Protection of Securities and Futures Industry*** mentions that the cross-border data transfer and personal information must be compliant with the provisions of ***the Cybersecurity Law*** and other relevant regulations. Securities and fund institutions shall also comply with ***the Cybersecurity Law*** and ***the Futures and Derivatives Law*** and other relevant regulations regarding the data transfer; the cross-border supervision and management of securities, futures etc. shall be conducted with the participation of the securities regulatory authority under the State Council, and securities regulatory authorities outside the Chinese mainland shall not directly conduct investigations, evidence collection and other activities within the Chinese mainland. Also, without the consent of securities regulatory authority under the State Council and the relevant competent authorities under the State Council, no enterprises or individuals shall transfer documents and materials relating to securities business activities and futures business activities outside the Chinese mainland without authorization.

Nevertheless, according to ***the Regulations on Cross-Border Data Flow***, the data processor is not required to submit Outbound Cross-Border Data Transfer Security

Assessment if such data is not notified or published as important data by competent authorities or in certain areas. However, it would be better for securities and fund enterprises to manage the data classification based on the foregoing provisions, and to adopt a more prudent attitude for cross-border data transfer that may involve the important data.

XLVI. What are the Common Scenarios of Cross-Border Data Transfer in the Pharmaceutical Industry?

In the pharmaceutical industry, cross-border data transfer is widely involved under different scenarios in the business operations of both Chinese enterprises developing overseas market and multinational enterprises cultivating the Chinese market. Such cross-border data transfer occurs in a wide range of scenarios, including R&D, marketing, commercialization, and cross-border licensing transactions.

Multi-regional clinical trials ("MRCTs") are very common in pharmaceutical R&D process. In MRCTs, trial data from different countries and regions is often collected based on similar clinical trial protocols, during which a large amount of clinical data is exchanged, shared, and transferred among different countries and regions and aggregated among various pharmaceutical enterprises. In addition to the aforementioned data and general personal information, data such as human genetic resources information is also involved. Moreover, under this scenario, pharmaceutical enterprises may also engage third-party service providers, such as electronic data capture providers (EDCs), to provide services such as data management, and the relevant servers may be located outside the Chinese mainland.

When submitting such as IND (Investigational New Drug) and NDAs (New Drug Submission) to overseas medical regulatory authorities, cross-border data transfer is also commonly involved. For example, under the IND scenario, documents such as research plans and research protocols may be submitted by Chinese entities to foreign drug regulatory authorities; and under the NDA scenario, various clinical data, case reports and relevant statistics may be submitted by Chinese entities to foreign drug regulatory authorities.

Under cross-border licensing transactions (License-in/License-out) in the

pharmaceutical industry, the licensees outside the Chinese mainland may, based on the licensing agreements with the Chinese licensors, require the Chinese licensors to provide the relevant IP and materials, which may include clinical trial data, materials and reports that have been kept by the Chinese licensors.

In addition, when participating in cross-border academic exchanges or sharing/releasing relevant clinical data to overseas institutions, cross-border data transfer may also be involved.

XLVII. What are the Types of Data Involved in Cross-Border Data Transfer in the Pharmaceutical Industry?

As discussed in the previous section, cross-border data transfer may occur under various scenarios in the pharmaceutical industry. From the regulatory perspective of the cyberspace authorities (considering that most enterprises are currently not regarded as CIIOs in practice), pharmaceutical enterprises need to identify the nature of the relevant data, so as to, together with other information, such as the amount of the data involved, determine which compliance procedure (e.g., submitting and passing the Outbound Cross-Border Data Transfer Security Assessment, submitting and recording submission of Standard Contract for Cross-Border Transfer of Personal Information, or conducting a Personal Information Protection Certification) they need to adopt. From the regulatory perspective of other government departments, it is also necessary to identify the specific compliance obligations that need to be fulfilled based on the nature of the data.

From the perspective of the regulation of data, enterprises may need to identify whether the data (to be) transferred is important data or core data. As discussed, pursuant to Article 2 of ***the Regulations on Cross-Border Data Flow***, the data processor is not required to apply for security assessment for cross-border data transfer if the data processor is not notified that the data is important data or the data is not publicly announced as important data. This provision reduces enterprises' compliance burden on identifying important data. Meanwhile, from the perspective of the regulation of personal information, pharmaceutical enterprises need to determine whether the amount of outbound transferred personal information falls into the different thresholds under ***the Regulations on Cross-Border Data Flow***, and whether such transfer involves

sensitive personal information.

As mentioned above, ***the Personal Information Protection Law*** defines sensitive personal information as "personal information that, once leaked or illegally used, will likely lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14". Appendix B of ***GB/T 35273-2020 Information Security Technology - Personal Information Security Specification*** enumerates certain types of sensitive personal information, including (i) individual's biometric information, such as genes, fingerprints, voiceprints, palm prints, auricle, iris, facial recognition features, etc., and (ii) individual's health and physical information, such as records related to the medical treatment of an individual, such as medical conditions, hospitalization records, medical orders, test reports, surgery and anesthesia records, nursing care records, medication records, drug and food allergy information, maternity information, past medical history, diagnosis and treatment condition, family medical history, current medical history, history of infectious diseases, etc.

It is important to note whether certain data is sensitive information depends on whether such data is personal information in the first place, i.e., "any kind of information related to an identified or identifiable natural person as electronically or via other means, excluding information that has been anonymized" as stipulated in ***the Personal Information Protection Law***. In clinical trials, the identities of subjects are generally de-identified by means of subject identification codes (their personal identities can be restored through corresponding unblinding measures). However, is such information still sensitive personal information after de-identification process? As discussed in previous sections, considering the current regulatory view of certain provincial-level CAC, the answer depends on whether such de-identification process can change the nature of "sensitivity". If the de-identified sensitive personal information is leaked or illegally used, and the leakage or illegal use will not result in the infringement of the natural person's human dignity or the endangerment of personal or property safety, then the de-identified sensitive personal information is no longer considered sensitive personal information. Since there is no clear official interpretation of "sensitivity" in the pharmaceutical industry, considering the characteristics of

pharmaceutical enterprises, some pharmaceutical enterprises choose to interpret such term in a strict way and regard the de-identified clinical trial data as sensitive personal information from a more prudent and conservation perspective.

In addition to the abovementioned perspectives, it is also necessary to identify the nature of the relevant cross-border data transfer according to regulations of the corresponding industry. The most important of which is human genetic resources information as stipulated in regulations such as ***the Administrative Regulations on Human Genetic Resources (the Regulations on Human Genetic Resources)***. According to *the Regulations on Human Genetic Resources*, human genetic resources information refers to the data and other information materials generated from the utilization of human genetic resources materials, while human genetic resources materials refer to the genetic materials with respect to organs, tissues, cells and so on which contain the human genome, genes and other genetic substances. ***The Implementation Rules for the Administrative Regulations on Human Genetic Resources*** further provide that human genetic resources information includes information materials such as human genes and genome data generated from the utilization of human genetic resource materials, and does not include clinical data, imaging data, protein data and metabolic data. The cross-border data transfer also involves in this special regulation of human genetic resources. Such information is often involved in scenarios such as clinical trials.

XLVIII. What are the Major Compliance Obligations for the Cross-Border Data Transfer for the Pharmaceutical Industry?

As discussed in the previous sections, from the regulatory perspective of the cyberspace authorities, pharmaceutical enterprises need to determine which compliance procedure they need to comply with (submitting and passing the Outbound Cross-Border Data Transfer Security Assessment, conducting and recording submission of Standard Contract for Cross-Border Transfer of Personal Information, or conducting a Personal Information Protection Certification) based on the specific nature of themselves, the nature of the cross-border data and other information such as the amount of the data transferred.

As we mentioned, in addition to determining whether it is a CIIO (currently, most enterprises are not regarded as CIIOs in practice), a pharmaceutical enterprise need to further assess from the perspectives of the amount and nature of the data, then determine the compliance procedure it shall undergo (For detailed content, please refer to "Part 1 Fundamentals: IV. What are the Three Routes for China's Current Outbound Cross-Border Data Transfer System? How Can One Determine Which Route to Select?"). Thanks to Article 2 of ***the Regulations on Cross-Border Data Flow***, burdens in terms of the supervision on "important data" on pharmaceutical enterprises have been reduced. However, as for the amount of personal data to be processed and the threshold of sensitive personal information, pharmaceutical enterprises still need to make their own determination according to the provisions of ***the Regulations on Cross-Border Data Flow***, and choose appropriate compliance procedures accordingly. Some enterprises with strong R&D capabilities may need to make a comprehensive judgment on whether they meet the threshold for security assessment for cross-border data transfer in scenarios such as clinical trials. While for some pharmaceutical enterprises that have limited operation and clinical trial scale and have not fully established their pipelines, they may need to enter into and record submission of Standard Contract for Cross-Border Transfer of Personal Information.

In addition, based on the provisions of ***the Personal Information Protection Law*** and other regulations, Chinese pharmaceutical enterprises may need to improve other compliance measures, such as (i) informing subjects and other relevant individuals of matters relating to the cross-border of their personal information and obtaining the individuals' specific consents (and updating documents such as their consent forms accordingly) in accordance with the provisions of ***the Personal Information Protection Law***; (ii) further strengthening the classification and grading management of the flow and processing of data, including the separate management of internal data and data from external suppliers and the classification of ordinary data and sensitive personal information; (iii) further strengthening the supervision and management of data compliance of overseas recipient, such as establishing a unified personal information and data management system within the group, adopting extensive technical measures such as de-identification and encryption, and requiring overseas recipient to enter into agreements with the relevant third party transferees to ensure that their personal information processing activities meet the standards of personal information protection

as provided in the relevant the Chinese mainland laws and regulations, etc.

From the perspective of the regulation of human genetic resources, pharmaceutical enterprises are also required to fulfill the relevant statutory obligations when conducting cross-border transfer of human genetic resources information.

According to ***the Administrative Regulations on Human Genetic Resources*** and other related regulations, foreign organizations and those institutions established or actually controlled by foreign organizations and individuals ("Foreign Entities") that intend to utilize China's human genetic resources to conduct scientific research activities (including clinical trials), shall cooperate with Chinese institutions, and shall report to the Human Genetic Resources Administration of China (the "HGRAC", Since May 1, 2024, the HGRAC has been reorganized from being a sub-section of the Ministry of Science and Technology to being a sub-section under the National Health Commission) for approval/recording submission. For a cooperation which involves the participation of Foreign Entities, either directly conducted by foreign organizations or by domestic institutions established/controlled by them, directly/indirectly sharing of human genetic resources with foreign entities could be involved.

For the cooperation process of conducting international cooperation in clinical trials, there are two routes for international cooperation scientific research, i.e., via approval of international cooperation in scientific research or recording submission of international cooperation clinical trial.

Specifically, when conducting an international cooperation clinical trial recording submission, the following conditions generally need to be fulfilled:

(1) The clinical trial (generally including Phase I, II and III clinical trials and bioequivalence tests (BE)) will be conducted to obtain a permit for the marketing of relevant drugs and medical devices in the PRC;

(2) No cross-border transfer of human genetic resource material will be involved.

(3) The clinical trial will be conducted in the clinical institutions by the utilization of the human genetic resources of China, and (a) the collection, testing, and analysis of the human genetic resources involved, the disposition of the residual human genetic resource materials, and related activities will be carried out within the clinical medical and health institution; or (b) the human genetic resources involved will be collected

within the clinical medical and health institution, and the testing, analysis, and disposition of the residual samples of the human genetic resources will be conducted by domestic entities designated under the clinical trial plans formulated to obtain a permit for the sale of relevant medicine or medical equipment.;

If the aforementioned conditions are all fulfilled, no approval of international cooperation in clinical trial is required, but only the prior recording submission with the HGRAC is required. If any of the above three conditions is not fulfilled, the path of international cooperation scientific research approval shall be chosen. In addition, parties of the clinical trial shall submit a report regarding the cooperation research to the HGRAC within 6 months after the completion of the international cooperation clinical trial.

Moreover, if human genetic resources information is cross-border transferred to the aforementioned Foreign Entities or is available for their use, the Chinese data owner shall also submit a prior report and backup of the information to the HGRAC. During clinical trials for which the aforementioned approval/recording submission has been obtained, if it has been agreed in the international cooperation agreement that the human genetic resources information generated shall be used by both parties, no separate prior report and the submission of the information backup is required. In addition, if a cooperation may affect China's public health, national security or social public interest in the abovementioned scenarios, the security review organized by the HGRAC is required.

In addition to the above provisions, there are also separate regulations and rules regulating from the perspective of healthcare big data, which pharmaceutical enterprises shall also pay attention to in the process of cross-border data transfer.

XLIX. What Cross-Border Data Compliance Issues Should be Considered for Cross-Border Data Trade through Domestic Data Exchanges?

According to China ICT Institute, the scale of China's digital economy will reach 56.1 trillion yuan in 2023, and the proportion of digital economy in GDP will be close to that of the secondary industry, accounting for more than 40 percent of the national

economy. Along with the rise of digital technology and the implementation of policies and laws related to the digital economy, cross-border digital trade with cross-border data flow as the underlying support has ushered in a booming development, which has profoundly changed the traditional international trade system.[33]

The channels of cross-border data trade are mainly divided into the data transactions in the data exchanges as cross-border trade platforms and the over-the-counter cross-border data trade carried out in a point-to-point model between the buyers and sellers of the data trades. Currently, China's data trading market is still in its infancy, and the volume of China's over-the-counter data trading accounts for about 95% of the overall data trading volume, while the scale of in-exchange trading is extremely small. [34]The point-to-point OTC direct transaction mostly relies on the conclusion of a trading contract, and the frequency of data flows herein is not high.

Regarding in-exchange transactions, the role of data exchanges in cross-border trade of data has gradually emerged, in the context of the background of policies and laws support and protection in China. As a leading data exchange, the Beijing Data Hosting Service Platform developed by the Beijing International Big Data Exchange was officially put into use in 2022, which is the China's first data hosting service platform that can support the enterprise cross-border data trade. Characterized with standardization, efficient management and customized services, it supports the provision of services such as data hosting, desensitized output, fusion computing and archiving and recording submission; the data hosting service platform in the pilot phase. The Shanghai Data Exchange actively expands its international data circulation and trading market. It has established a co-operation mechanism for the two-way flow of data with overseas platforms, established an international board, which is an innovation of the business model of "data exchange + global digital platform". The Shenzhen Data Exchange has also achieved a series of innovative and exemplary results in cross-border data trading and actively explored cross-border data pilots. Adjacent to Hong Kong and Macao, Shenzhen Data Exchange has deployed its unique geographical advantage of being located in the Guangdong-Hong Kong-Macao Greater Bay Area and has successfully released the first cross-border data transaction in the exchange.

---

[33] See *the Research Report on the Development of China's Digital Economy (2023)* by the China Academy of Information and Communications Technology.
[34] Titanium Media: *China's digital economy is entering a new stage*.

Given cross-border data trading in-exchange involves cross-border data flow, such data trades also involve data outbound compliance. From a legal approach, as the current domestic law does not specifically provide for any compliance exemption mechanism for those outbound data trades via the exchanges, the cross-border data trades through data exchanges shall also comply with the existing cross-border data transfer laws and regulations and fulfill the compliant requirements regarding cross-border data transfer. In addition, data exchanges, as trading platforms, will also independently conduct data compliance review and security checks on the data products for outbound trade, and require the data providers to provide compliance review reports issued by a third-party professional entity (e.g. law firm).

For example, according to our research on public information, the first in-exchange outbound data transaction via Shenzhen Data Exchange is the "SmarTag News Analysis Data" product provided by ChinaScope (Shanghai) Technology Enterprise. As the "self-proof" materials for the transaction, this enterprise provided to Shenzhen Data Exchange the information collection form, basic information on the subject matter of the transaction, the parties to the transaction, the transaction scenario, data security and other transaction information, and also the corresponding materials for the submission and approval required by the national and local relevant departments (e.g. data security review data, outbound security assessment). In addition, this data product provider also engaged a professional law firm to issue a legal opinion on the compliance assessment of the transaction, in order to disclose the compliance risks in the data transaction. This opinion has been provided to Shenzhen Data Exchange alongside the "self-proof" materials as third-party proof materials. On the basis of the self-proof and third-party proof materials provided by this seller, Shenzhen Data Exchange submitted a large scale of compliance assessments on data outbound processing, circulation, management, technical measures, compliance and legality, data security, etc. Finally, five data transactions with a total amount of nearly RMB 5 million yuan were concluded.

L. Can Public Data Operators Authorize or Share Public Data with Overseas Entities?

According to ***Data Twenty Articles***, data is categorized into public data, corporate data, and personal data[35]. As per ***Data Twenty Articles*** and various local government data regulations and administrative laws and rules related to public data operations, public data refers to data generated in the course of legal duties or provision of public services by party and government agencies at all levels, and enterprises and institutions. In the context of public data operations, another issue arises: since the operation of public data in all regions should adhere to the principle of "original data remains within the domain, data is usable but not visible," the public data discussed by public data operators is generally no longer the original data or merely preliminary governed public data resources, but involves public data products in the phase of authorized use or conditional sharing and openness.[36]

According to the local data ordinances in many provinces and municipalities as well as the administrative rules and regulations related to the authorized operation of public data, upon the condition that data compliance and security is satisfied, the public data can be authorized for external use or sharing. In particular, many provincial and municipal local governments have adopted the conditional use or sharing conditions on top of the public data classification rules. However, Article 20 of ***the Data Twenty Articles*** also provide that, based on the requirement of personal privacy protection and public safety, while encouraging public data utilization, it is also required that the public data operators/data product developer shall comply with the requirement that the "original data does not go out of the domain, the data is available but not visible", e.g. providing data products or services to the society in the manner of data models, verification technology, etc.. Under such requirement, one question would arise as whether a legal entity located outside the Chinese mainland (in particular, overseas enterprises that need public data from China to train their models) can become an authorized user or can obtain the public data through the public data open and share

[35] *Opinions on Establishing a Data Infrastructure to Better Leverage the Role of Data as an Economic Factor* (Part 3): Explore the structural separation of data property rights. Establish a classified and graded authorization system for public data, corporate data, and personal data. — Central Committee of the Communist Party of China, State Council "Opinions on Building Data Infrastructure to Better Leverage Data as an Economic Factor." Central Documents on China Government Website (www.gov.cn).

[36] The concept of data products mentioned here is in a broad sense, encompassing but not limited to statistical data, datasets, data services, data applications, and data products. This includes data products and services provided to society in forms such as models, verifications, and other similar formats.

mechanism?

This is a complex issue, and it requires a case-by-case analysis pending on the specific public data operation mode in each case. Currently, there are no restrictions under the existing laws and regulations. Therefore, in theory, with the satisfaction of the requirements of legal compliance and data security, the overseas legal entities can also obtain public data within the territory of the country by taking legitimate and feasible technical means.

From a legal perspective, the following key data compliance issues shall be noted and considered by such overseas legal entities:

Firstly, according to ***the Regulations on Cross-Border Data Flow***, public data obtained by overseas legal entities fall into the category of data cross border transfer. Therefore, for such public data transaction, the corresponding data outbound compliance requirements in accordance with ***the Regulations on Cross-Border Data Flow*** shall be fulfilled, taking into account the specific scenarios and products.

Secondly, for public data to be exported, it is recommended that a data security review should also be conducted, i.e. whether the public data to be exported contain sensitive information such as core data, state secrets, important data, or information relating to national security shall be assessed. If it does, data transfer shall not be allowed, or the data security review and compliant rectification measures shall be taken prior to data transfer. In addition, according to the corresponding provisions of the DSL, even if an overseas entity is legally qualified to obtain public data, other legal compliance requirements and restrictive requirements such as local storage of data and export control would be triggered. For specific details, please refer to the corresponding sections of this Practice Handbook.

In the event that the public data contains personal information and the corresponding personal information will go beyond the original purpose and scope at the time of original public data collection and the scope of authorized use, the cross border transfer of the data itself will call for the fulfillment of the corresponding compliance requirements pursuant to ***the Personal Information Protection Law*** (such as informing the individual and obtaining separate consent for the data cross border transfer). For details, please refer to the corresponding questions in this Practice Handbook. Nevertheless, we can foresee that as such notification and consent would

require effective channels to interact with individuals, it would not be practical in the public data domain to accomplish such tasks. In addition, public data operators and foreign entities must sign a data authorization or data sharing agreement to agree on and facilitate sufficient protection for the data provider and the data. In particular, the agreement must explicitly stipulate that, without the consent of the data provider, the overseas entity shall not transfer, share or authorize the data for further use by a third party, in order to protect the safe use of public data.

In addition, as public data operator must conduct data operation activities in strict accordance with the requirement that “original data must remain in the domain, data should be available but not visible”, the overseas entity may be required to obtain the data or data results physically on the platform operated by public data operator, through the deployment of privacy computing, sandbox or other technological measures. In this regard, it is possible that overseas entities may need to deliver its data model to the public data operator. This thus may likely trigger the cross-border data compliance requirements and possible restrictions in the overseas entity’s jurisdiction. Further, after the data model is fused with with “usable but invisible” data, new data compliance issues derived from how the data results can be brought back to its home country in a lawful and secure manner would arise.

As the cross-border transfer of public data involves both data compliance issues in the public data domain and data outbound compliance issues, we recommend that both the public data operators and overseas entities shall sufficiently consult professional legal advisers at an early stage when encountering similar issues.

Annex I. The National and Provincial Cyberspace Administration Contact Information

Cyberspace Administration	Address	Contact Number
the Cyberspace Administration of China	No.11 Chegongzhuang Street, Xicheng District, Beijing	Submitting the cross-border data transfer security assessment: 010-55627135
		Record Submission of Standard Contract for Cross-Border Transfer of Personal Information 010-55627565
		Conducting the Personal Information Protection Certification: 010-82261100
the Cyberspace Administration of Beijing Province	No. 413, Hongshan Home, South Huawei Road, Chaoyang District, Beijing, China	010-67676912
the Cyberspace Administration of Tianjin Province	No.20 Meijiang Road, Hexi District, Tianjin, China	022-88355322
the Cyberspace Administration of Hebei Province	No. 79, Weiming South Street, Qiaoxi District, Shijiazhuang City, Hebei Province, China	0311-87909716
the Cyberspace Administration of Henan Province	No. 16, Jinshui Road, Jinshui District, Zhengzhou City, Henan Province, China	0371-65901067
the Cyberspace Administration of Zhejiang Province	No. 29, Provincial Government Road, Xihu District, Hangzhou, Zhejiang Province, China	0571-81051250
the Cyberspace Administration of	No. 315, Wanping Road, Xuhui	021-64743030-2711

Cyberspace Administration	Address	Contact Number
Shanghai Province	District, Shanghai, China	
the Cyberspace Administration of Jiangsu Province	No. 8, Bailongjiang East Street, Jianye District, Nanjing, Jiangsu Province, China	025-63090194
the Cyberspace Administration of Fujian Province	No. 133, Beidai Road, Gulou District, Fuzhou City, Fujian Province, China	0591-86300613
the Cyberspace Administration of Anhui Province	No.1 Zhongshan Road, Baohu District, Hefei City, Anhui Province, China	0551-62606014
the Cyberspace Administration of Chongqing Province	No. 6, Qingzhu East Road, Yubei District, Chongqing, China	023-63151805
the Cyberspace Administration of Guizhou Province	No. 39, Baoshan North Road, Yunyan District, Guiyang City, Guizhou Province, China	0851-82995001/ 82995061
the Cyberspace Administration of Shandong Province	No. 20637, Jingshi Road, Shizhong District, Jinan City, Shandong Province, China	0531-51773249/ 51771297
the Cyberspace Administration of Guandong Province	No. 104, Zhongshan Yi Road, Yuexiu District, Guangzhou City, Guangdong Province, China	020-87100794/ 87100793
the Cyberspace Administration of Shanxi Province	No. 10, South Yanta Road, Yanta District, Xi’an, Shaanxi Province, China	029-63907136
the Cyberspace Administration of Gansu Province	No.1648, Nanchang Road, Chengguan District, Lanzhou City, Gansu Province, China	0931-8928721
the Cyberspace Administration of Shanxi Province	No.36, Wuyi Road, Yingze District, Taiyuan City, Shanxi Province, China	0351-5236020

Cyberspace Administration	Address	Contact Number
the Cyberspace Administration of Jiangxi Province	No. 999, Wolong Road, Honggutan District, Nanchang, Jiangxi, China	0791-88912737
the Cyberspace Administration of Yunan Province	No. 516, Rixin Middle Road, Xishan District, Kunming, Yunnan Province, China	0871-63902424
the Cyberspace Administration of Hubei Province	No. 268, Fruit Lake Road, Wuchang District, Wuhan City, Hubei Province, China	027-87231397
the Cyberspace Administration of Hunan Province	No.1 Shaoshan North Road, Furong District, Changsha, Hunan Province, China	0731-81121089
the Cyberspace Administration of Qinghai Province	No. 32, Wenjing Street, Haihu New District, Xining City, Qinghai Province, China	0971-8485510
the Cyberspace Administration of Liaoning Province	No.26A Guangrong Street, Heping District, Shenyang, Liaoning Province, China	024-81680082
the Cyberspace Administration of Jilin Province	No. 666 Xinfa Road, Chaoyang District, Changchun City, Jilin Province, China	0431-82761087
the Cyberspace Administration of Heilongjiang Province	No. 12, Huashan Road, Nangang District, Harbin City, Heilongjiang Province, China	0451-58685723
the Cyberspace Administration of Hainan Province	No. 69, Guoxing Avenue, Haikou City, Hainan Province, China	0898-65380723
the Cyberspace Administration of Sichuan Province	No.21 Guihua Lane, Qingyang District, Chengdu, Sichuan Province, China	028-86601862
the Cyberspace Administration of	No. 112, Minzu Avenue, Qingxiu District, Nanning City,	0771-2093017/ 2093049

Cyberspace Administration	Address	Contact Number
Guangxi Zhuang Autonomous Region	Guangxi Zhuang Autonomous Region, China	
the Cyberspace Administration of Ningxia Hui Autonomous Region	No.1 Kangping Road, Jinfeng District, Yinchuan City, Ningxia Hui Autonomous Region, China	0951-6668938
the Cyberspace Administration of Tibet Autonomous Region	No.7, Nongke Road, Chengguan District, Lhasa, Tibet Autonomous Region, China	0891-6591509
the Cyberspace Administration of Inner Mongolia Autonomous Region	No.8, Yinhe South Street, Saihan District, Hohhot City, Inner Mongolia Autonomous Region, China	0471-4821277
the Cyberspace Administration of Xinjiang Uighur Autonomous Region	No. 2221, Xihuan North Road, New Downtown, Urumqi, Xinjiang Uygur Autonomous Region	0991-2384855
the Cyberspace Administration of Xinjiang Production and Construction Corps	No. 462, Zhongshan Road, Tianshan District, Urumqi City, Xinjiang Uygur Autonomous Region	0991-2899091

Annex II. Glossary Reference

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
数据出境	outbound data transfer	/	/
个人信息出境	outbound personal information transfer	/	/
数据跨境传输	cross-border data transfer	/	/
数据跨境流动	cross-border data flow	/	/
数据出境安全评估	Outbound Cross-Border Data Transfer Security Assessment	/	/
数据出境安全评估申报	Outbound Cross-Border Data Transfer Security Assessment Submission	/	/
数据出境风险自评估	Outbound Cross-Border Data Transfer Risk Self-Assessment	/	/
数据出境风险自评估报告	Outbound Cross-Border Data Transfer Risk Self-Assessment Report	/	/
数据出境风险自评估报告（模板）	Outbound Cross-Border Data Transfer Risk Self-Assessment Report (Template)	/	/
数据跨境传输评估	Data Transfer Impact Assessment	/	DTIA
关键信息基础设施运营者	Critical Information Infrastructure Operators	/	CIIO
个人信息保护认证	Personal Information Protection Certification	/	/
个人信息保护影响评估	Personal Information Protection Impact Assessment	/	PIA

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
数据处理协议	Data Processing Agreement	/	DPA
自由贸易试验区负面清单制度	Negative List for Pilot Free Trade Zone	/	FTZ negative list
敏感个人信息	Sensitive Personal Information	/	/
单独同意	separate consent	/	/
认证主体	certification applicant	/	/
中国（上海）自由贸易试验区	China (Shanghai) Pilot Free Trade Zone	上海自贸区	/
粤港澳大湾区	Guangdong－Hong Kong－Macao Greater Bay Area	/	the Greater Bay Area (GBA)
中华人民共和国香港特别行政区、中华人民共和国澳门特别行政区、中华人民共和国台湾地区的统称	Hong Kong, Macao and Taiwan regions of China	港澳台地区	/
个人信息出境标准合同	the Standard Contract for the Outbound Transfer of Personal Information	/	/
个人信息保护影响评估报告	Personal Information Protection Impact Assessment Report	/	/
个人信息保护影响评估报告（模板）	the Personal Information Protection Impact Assessment Report (Template)	/	/
数据处理者	data processor	/	/
境外接收方	overseas recipient	/	/
豁免情形	exemptions	/	/

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
核心数据	core data	/	/
重要数据	important data	/	/
一般数据	general data	/	/
个人信息出境标准合同备案	Record Submission of Standard Contract for Cross-Border Transfer of Personal Information	/	/
统一社会信用代码	the Uniform Social Credit Code	/	/
个人信息处理者/认证委托人	the personal information processer/the certification applicant	/	/
境内	within the Chinese mainland	/	/
境外	outside the Chinese mainland	/	/
征求意见稿	Draft for Comment	/	/
个人信息主体	personal information subject	/	/
明示同意	explicit consent	/	/
匿名化	anonymization	/	/
去标识化	de-identification	/	/
个性化展示	personalized display	/	/
《数据出境合规实务 50 问》	Outbound Cross-Border Data Transfer Compliance Guideline: 50 Common Questions	《实务问答》	Practical Q&A
《中华人民共和国网络安全法》	Cybersecurity Law of the People’s Republic of China	《网络安全法》	The Cybersecurity Law

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
《中华人民共和国个人信息保护法》	Personal Information Protection Law of the People's Republic of China	《个人信息保护法》	The Personal Information Protection Law
《中华人民共和国数据安全法》	Data Security Law of the People's Republic of China	《数据安全法》	The Data Security Law
《中华人民共和国刑法》	Criminal Law of the People's Republic of China	《刑法》	The Criminal Law
《中华人民共和国保守国家秘密法》	State Security Law of the People's Republic of China	《保守国家秘密法》	The State Security Law
《中华人民共和国测绘法》	Surveying and Mapping Law of the People's Republic of China	《测绘法》	The Surveying and Mapping Law
《中华人民共和国生物安全法》	Biosecurity Law of the People's Republic of China	《生物安全法》	The Biosecurity Law
《中华人民共和国出入境管理法》	Exit and Entry Administration Law of the People's Republic of China	《出入境管理法》	The Exit and Entry Administration Law
《中华人民共和国证券法》	Securities Law of the People's Republic of China	《证券法》	The Securities Law
《中华人民共和国期货和衍生品法》	Futures and Derivative Law of the People's Republic of China	《期货和衍生品法》	The Futures and Derivative Law
《数据出境安全评估办法》	the Measures for the Security Assessment of Cross-Border Data Transfer	《出境评估办法》	the Assessment Measures for Data Transfer
《信息安全技术 数据出境安全评估指南（征求意见稿）》	the Information Security Technology- Guidelines for Cross-border Data Transfer Security Assessment (Draft for Comment)	《安全评估指南（征）》	the Guidelines for Security Assessment (Draft)

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
《网络数据安全管理条例》	the Regulations on Network Data Security Management	《网数条例》	the Network Security Management Regulations
《网络数据安全管理条例（征求意见稿）》	the Regulations on Network Data Security Management (Draft for Comment)	《网数条例（征）》	the Network Security Management Regulations (Draft)
《关于实施个人信息保护认证的公告》	the Announcement on the Implementation of Personal Information Protection Certification	《认证公告》	the Certification Announcement
《个人信息保护认证实施规则》	the Certification for Personal Information Protection Implementation Rules	《认证规则》	the Certification Rules
《个人信息出境个人信息保护认证办法（征求意见稿）》	the Measures for the Certification of Personal Information Protection for Outbound Personal Information Transfer(Draft for Comment)	《认证办法（征）》	the Certification Measures for Outbound Personal Information Transfer (Draft)
《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》	the Guidelines to Cybersecurity Standards - Specification on Security Authentication for Cross-Border Personal Information processing Activities	《认证规范 V1.0》	the Certification Specification V1.0
《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》	the Guidelines to Cybersecurity Standards - Specification on Security Authentication for Cross-Border Personal Information processing Activities V2.0	《认证规范 V2.0》	the Certification Specification V2.0
《信息安全技术 个人信息跨境传输认证要求（征求意见稿）》	Information Security Technology - Certification Requirements for Cross-Border Transfer of Personal Information (Draft for Comment)	《跨境认证要求（征）》	the Certification Requirements for Cross-Border Transfer (Draft)

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
《关于促进粤港澳大湾区数据跨境流动的合作备忘录》	the Memorandum of Cooperation on Promoting Cross-Border Data Flow in the Guangdong-Hong Kong-Macao Greater Bay Area	/	/
《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》	the Guidelines to Cybersecurity Standards - Requirements for Protection of Cross-border Personal Information in Guangdong-Hong Kong-Macao Greater Bay Area (Draft for Comment)	/	/
《个人信息出境标准合同办法》	the Measures for the Standard Contract for Cross-border Transfer of Personal Information	《标准合同办法》	the Measures for the Standard Contract
《促进和规范数据跨境流动规定》	the Regulations on Promoting and Regulating Cross-Border Data Flow	《跨境流动规定》	the Regulations on Cross-border Data Flow
《数据出境安全评估申报指南（第二版）》	the Guidelines to Submission for Security Assessment of Outbound Data Transfers (Second Edition)	《评估申报指南（第二版）》	the Guidelines to Assessment Submission (Second Edition)
《个人信息出境标准合同备案指南（第二版）》	the Guidelines to Recording Submission of Standard Contract for Outbound Cross-border Transfer of Personal Information (Second Edition)	《标准合同备案指南（第二版）》	the Guidelines to Recording Submission of Standard Contract (Second Edition)
《数据出境申报系统使用说明（第一版）》	the Instructions for Outbound Data Transfer Submission System (First Edition)	/	/
GB/T 35273-2020《信息安全技术 个人信息安全规范》	GB/T 35273-2020 Information Security Technology - Personal Information Security Specification	/	/

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	GB/T 39335-2020 Information Security Technology - Guidelines to Personal Information Security Impact Assessment	/	/
GB/T 43697-2024《数据安全技术 数据分类分级规则》	GB/T 43697-2024 Data Security Technology — Rules for Data Classification and Grading	/	/
《重要数据识别指南》	Guidelines for the Identification of Important Data	/	/
香港《个人资料（私隐）条例》	the Personal Data (Privacy) Ordinance of Hong Kong	/	/
《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	Implementation Guidelines for the Standard Contract for Cross-Border Flow of Personal Information in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)	《实施指引》	Implementation Guidelines
《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) Personal Information Cross-border Flow Standard Contract	《大湾区标准合同》	GBA Standard Contract
《信息安全技术 个人信息安全影响评估指南》	GB/T 39335 -2020 Information Security Technology - Guidelines for Personal Information Security Impact Assessment	/	/
《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》	the Measures for Classification and Grading of Cross-Border Data Flow in Lingang Special Area of China (Shanghai) Pilot Free Trade Zone (for Trial Implementation)	/	/

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
《征信业务管理办法》	the Measures for the Administration of the Credit Reporting Business	/	/
《中国人民银行业务领域数据安全管理办法（征求意见稿）》	the Measures for Data Security Management in the Business Sector of the People's Bank of China (Draft for Comment)	/	/
《个人金融信息保护技术规范》	the Personal Financial Information Protection Technical Specification	/	/
《金融数据安全 数据安全分级指南》	the Financial Data Security—Guidelines for Data Security Classification	/	/
《金融数据安全 数据生命周期安全规范》	the Financial Data Security—Security Specification of Data Life Cycle	/	/
《证券期货业数据分类分级指引》	the Guidance for Data Classification of Securities and Futures Industry	/	/
《证券期货业数据安全管理与保护指引》	the Guidance for Data Security Management and Protection of Securities and Futures Industry	/	/
《证券期货业数据安全风险防控 数据分类分级指引》	Data Security Risk Prevention and Control for Securities and Futures Industry — Guidelines on Data Classification	/	//
《人类遗传资源管理条例》	Administrative Regulations on Human Genetic Resources	《人遗条例》	Regulations on Human Genetic Resources
《人类遗传资源管理条例实施细则》	Implementation Rules for the Administrative Regulations on Human Genetic Resources	《人遗细则》	Implementation Rules on Human Genetic Resources

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》	Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Data Base System and Better Utilizing the Role of Data Elements	《数据二十条》	Twenty articles of data
《国家健康医疗大数据标准、安全和服务管理办法（试行）》	the Measures for the Management of National Healthcare Big Data Standards, Security and Services (for Trial Implementation)	/	/
《上海市落实〈全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案〉的实施方案》	Shanghai Municipal's Implementation Plan of the Overall Program for Comprehensively Connecting with International High-standard Economic and Trade Rules and Promoting High-level Institutional Liberalization of China (Shanghai) Pilot Free Trade Zone	《上海开放实施方案》	Implementation Plan for the opening up of Shanghai
《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》	the Measures for Classification and Grading of Cross-Border Data Flow in Lingang Special Area of China (Shanghai) Pilot Free Trade Zone (for Trial Implementation)	/	/
中华人民共和国国务院，即中央人民政府	The State Council of the People's Republic of China	国务院	/
中华人民共和国国务院科学技术主管部门	Department of Science and Technology of the State Council of the People's Republic of China	国务院科学技术主管部门	/
国家互联网信息办公室	the Cyberspace Administration of China	国家网信办	CAC

Chinese Expression	English Expression	Chinese Abbreviation	English Abbreviation
中华人民共和国科技部	Ministry of Science and Technology of the People´s Republic of China	/	/
中华人民共和国公安部	Ministry of Public Security of the People's Republic of China	/	/
中华人民共和国国家安全部	Ministry of State Security of the People's Republic of China	/	/
中华人民共和国工业和信息化部	Ministry of Industry and Information Technology of the People's Republic of China	/	/
中华人民共和国司法部	Ministry of Justice of the People's Republic of China	/	/
全国网络安全标准化技术委员会	the National Technical Committee 260 on Cybersecurity of Standardization Administration of China	网安标委	TC260
国家市场监督管理总局	State Administration for Market Regulation	/	/
中国网络安全审查认证和市场监管大数据中心	China cybersecurity review, certification and market regulation big data center	/	CCRC
中国人类遗传资源管理办公室	Human Genetic Resource Administration of China	人遗办	HGRAC
中国信息通信研究院	China Academy of Information and Communications Technology	中国信通院	/
中华人民共和国国家监察委员会	the National Commission of Supervision of the People's Republic of China	/	/

EDITORS

Xu Guosheng Cao Ying

TRANSLATORS

(IN NO PARTICULAR ORDER AND IN ALPHABETICAL ORDER OF NAMES)

Cao Ruanhui	Dong Jierui	Liu, Jerry (Zhan)
Li, Lilian (Ling)	Liang Xinyi	Meng, Maggie (Jie)
Shi, Ethan (Yi)	Tian, Leo (Liang)	Wu, Wendy (Yongheng)
Wu, Charles (Junkun)	Yao Ping	Zhang, James (Tong)
Zhang Sijing	Zhang, TJ (TianJing)	Zhang Yang

CO-PUBLISHERS AND AUTHORS OF THE CHINESE VERSION

GLOBAL LAW OFFICE

Meng, Maggie (Jie)	Liu, Jerry (Zhan)	Li, Lilian (Ling)
Zhang, James (Tong)	Lin Yi	Tian Ziyi
Wang Zixuan		

UNIVERSITY OF INTERNATIONAL BUSINESS AND ECONOMICS RESEARCH CENTER FOR DIGITAL ECONOMY AND LEGAL INNOVATION

Xu Ke

NIO HOLDINGS LTD.

Gao Gang Wang Shisun

QI AN XIN TECHNOLOGY GROUP INC.

Ma Lan Liu Qianwei Liu Hongliang

BEIJING OGILVYONE MARKETING CO., LTD.

Jack Yin

HANGZHOU YOUZAN TECHNOLOGY CO., LTD.

Fang Ziwen Chen Xin Wei Dongjie

OTHER AUTHORS

Guo Juntong Tian Leo (Liang) Wang Cheng

Dong Jierui Yin Tonghui

Please scan the QR code to obtain the Chinese version of Outbound Cross-Border Data Transfer Compliance Guideline: 50 Common Questions (2024 Edition)

Disclaimer

This document does not represent the legal opinions of all jointly issuing units on relevant issues. Any decisions on actions or inactions made solely based on all or part of the content of this document, as well as the consequences resulting therefrom, shall be the sole responsibility of the actor.If you need legal advice or ther professional advice, you should seek professional assistance from qualified professionals.

Copyright

Contact

E. dataprotection@glo.com.cn