PILLAR LEGAL

Security Assessment for Cross-Border Data Transfers

CHINA REGULATION WATCH[1]

July 20, 2022

By: Zhu Ziwei | Alexandra Ashbrook

1. Introduction

On July 7, 2022, the Cyberspace Administration of China (国家互联网信息办公室)("CAC") released the final version of the Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法) (the "Security Assessment Measures"). The Security Assessment Measures set forth requirements for the transfer of personal information and important data collected within the territory of People's Republic of China ("China" or "PRC") out of China after passing a security assessment conducted by the CAC.

The CAC security assessment was first raised in the Cyber Security Law (网络安全法),[2] and is aimed at supervising any cross-border transfers of personal information and important data by critical information infrastructure operators.[3] Later, the Personal Information Protection Law (个人信息保护法) ("PIPL"), effective on November 1, 2021, adopted this CAC security assessment mechanism for cross-border transfers of personal information by critical information infrastructure operators and personal information processors whose processing of personal information reaches certain threshold amounts prescribed by the CAC.[4] Apart from the strict CAC security assessment, there are two other approaches that allow companies to transfer a relatively small portion of less sensitive personal information to overseas recipients under PIPL: entering into a standard contract provided by CAC[5] or obtaining a personal information

【博申津師事務所】

[1] This China Regulation Watch is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This China Regulation Watch may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-930-3932 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: info@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] The Cyber Security Law (网络安全法) was issued by the Standing Committee of the National People's Congress (全国人大常委会) on November 7, 2016 and became effective on June 1, 2017.

[3] Pursuant to Article 37 of the Cyber Security Law, personal information and important data collected and generated by critical information infrastructure operators during their operations within the territory of China shall be stored in China. If it is necessary to provide such information and data to overseas recipients, a security assessment shall be conducted in accordance with the measures developed by CAC in conjunction with relevant departments of the State Council (国务院).

[4] Pursuant to Article 40 of PIPL, critical information infrastructure operators, or personal information processors whose processing of personal information reaches the threshold amount prescribed by CAC, shall store in China the personal information collected or generated by them within the territory of China. Where it is necessary to provide such information to an overseas recipient, a security assessment conducted by CAC shall be passed.

[5] You may find more information in our China Regulation Watch: Standard Contract for Cross-Border Transfers of Personal Information.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

protection certification issued by a third-party professional agency.[6] Although these requirements for cross border transfers of personal information became effective with PIPL on November 1, 2021, the CAC is just now providing details of how to implement such requirements with the issuance of the Cross-Border Personal Information Processing Security Certification Specifications (个人信息跨境处理活动安全认证规范) on June 24, 2022 (the "Certification Specifications"), the draft Personal Information Cross-Border Transfer Standard Contract Provisions (个人信息出境标准合同规定) on June 30, 2022 (the "Draft Standard Contract Provisions") and the Security Assessment Measures on July 7, 2022.

2. Applicable Situations

Although the CAC security assessment is often discussed in the context of transferring personal information out of China, any transfers of important data out of China also requires a CAC security assessment. "Important data" means any data, once tampered with, damaged, leaked or illegally acquired or used, may endanger China's national security, the operation of China's economy, social stability, public health, or security.[7] It usually does not include any personal information, however statistical data and derivative data generated from massive personal information processing activities may also be regarded as important data.[8] The Data Security Law (数据安全法) requires relevant government departments to provide lists of categories of data considered "important data" for different industries, but currently only the Vehicle Data Security Management Provisions (for Trial Implementation) (汽车数据安全管理若干规定（试行）)[9] list out specific categories of important data relevant to the vehicle industry.[10]

According to Article 4 of the Security Assessment Measures, the cross-border security assessment will apply in the following situations:

- Transferring any important data out of China;
- Transferring any personal information out of China by a critical information infrastructure operator or a data processor that processes the personal information of more than 1,000,000 individuals; or
- Transferring any personal information out of China by a data processor that provides personal information of more than 100,000 individuals or provides sensitive personal information of more than 10,000 individuals to overseas recipients as of January 1 of the previous year.

---

[6] You may find more information in our China Regulation Watch: Cross-Border Personal Information Processing Security Certification Specifications.

[7] See Article 19 of the Security Assessment Measures.

[8] See Section 2 of the Guidelines on Internet Data Classification and Grading (网络数据分类分级指引) issued by the National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会) in December 2021.

[9] The Vehicle Data Security Management Provisions (for Trial Implementation) (汽车数据安全管理若干规定（试行）) was jointly issued by CAC, the National Development and Reform Commission (国家发展和改革委员会), the Ministry of Industry and Information Technology (工业和信息化部), the Ministry of Public Security (公安部), and the Ministry of Transport (交通运输部门) on August 18, 2021, effective on October 1, 2021.

[10] Important data in vehicle industry will include geographical information, flows of people or vehicles and other data related to military districts and any other important sensitive areas; traffic volume, logistics and other data that reflect performance of the economy; operating data of a vehicle charging network.

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932

Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206

www.pillarlegalpc.com

Note that the threshold amounts mentioned above are easily crossed given the large population of China, because the number is calculated by measuring the number of individuals (i.e., personal information subjects) whose personal information is processed by the data processor as a whole, as opposed to in different instances or to different overseas recipients.

The Security Assessment Measures provide a compliance grace period of six months for cross-border data transfers already carried out before the effective date, September 1, 2022. But for cross-border data transfers occurring after September 1, 2022, the CAC security assessment must be completed before any transfer activity.[11]

3. Requirements of Applying for Security Assessment

Before applying for a cross-border data transfer security assessment, the applicant for such assessment must first conduct a self-assessment of the risks involved with such transfer, focusing in particular on the potential risks to China's national security and public interests. With respect to cross-border transfers of personal information, the personal information protection impact assessment ("PIPIA") under PIPL satisfies the self-assessment requirement.[12] The applicant must submit to a CAC local office (i) an application form, (ii) a self-assessment report, (iii) a data processing agreement by and between the data processor and the overseas recipient, and (iv) other materials as required for a security assessment.

The results of a CAC security assessment are valid for 2 years, and the applicant must apply for new security assessment 60 working days before the previous assessment expires. However, even during the valid period, the applicant may need to apply for a new security assessment if any of the following conditions occur:

- There is any change to the purpose, method, scope, type of the data transferred, or change to the purpose or method of data processing activities by the overseas recipient which may affect the security of data transferred;
- The retention period of personal information or important data is prolonged;
- There is any change in data security protection policies, legislation, the cybersecurity environment, or any other force majeure event occurs in the country or region where the overseas recipient is located that may affect the security of data transferred;
- There is any material change in the actual control or business scope of the overseas recipient that may affect the security of data transferred; or
- Other circumstances exist that may affect the security of data transferred.

4. Security Assessment Procedure and Criteria

The local CAC office will conduct a completeness check of the submitted documents within 5 working days of submission. If no additional materials are required, the local office will submit the documents to the CAC. Thereafter, CAC will issue a notice of receipt to the applicant within 7 working days after receiving the documents from the local office. CAC will then

[11] See Article 20 of the Security Assessment Measures.

[12] PIPIA is a process designed to help identify, analyze and mitigate the risks associated with certain personal information processing activities, which is similar to the data protection impact assessments ("DPIA") provided for under the European Union's General Data Protection Rules ("GDPR").

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932

Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206

www.pillarlegalpc.com

complete a material assessment of the documents within 45 days after issuing the notice of receipt, unless the case is complicated or there is a need for any supplementary materials or corrections.[13]

The CAC security assessment will focus on the following matters:

- The legality, legitimacy, and necessity of the cross-border data transfer;
- The purpose, scope, method, and other aspects related to the data processing by the overseas recipient;
- The impact that the data security protection policies and legislation and cybersecurity environment of the country or region where the overseas recipient is located may have on the security of the data to be transferred; whether the data protection level of the overseas recipient meets the requirements and standards of China;
- The quantity, scope, type, and sensitivity of the data to be transferred, and the risks that such data being tempered with, damaged, leaked, lost, relocated or illegally acquired or used during and after the cross-border data transfer;
- Whether data security and personal information rights and interests can be sufficiently and effectively ensured;
- Whether data security protection obligations are sufficiently stipulated in the data processing agreement between the data processor and the overseas recipient;
- The compliance with China's laws, regulations and departmental rules; and
- Other matters to be assessed as deemed by CAC.[14]

If application fails to pass the security assessment, the applicant may apply for reassessment within 15 working days after receiving the results from the CAC. However, the results of any such reassessment are final. In addition, if an applicant submits false materials, the CAC will reject the application and the applicant will be held legally liable under applicable laws.

5. Comparison of Three Approaches to Cross-Border Transfers of Personal Information

Among the three approaches to cross-border transfers of personal information promulgated under PIPL, the CAC security assessment is currently the only approach supported by confirmed rules issued by a government authority with legislative power. The Draft Standard Contract Provisions associated with the CAC's standard contract approach are still in draft form and may change pursuant to public comments. Similarly, the Certification Specifications were issued by the Secretary of National Information Security Standard Technology Committee (全国信息安全标准化技术委员会秘书处), a non-legislative body. Regardless, below is a comparison of the applicable situations, required materials, and procedures for the three approaches to personal information cross-border transfers, based on the currently available materials.

[13] Rules in China often impose deadlines on government departments when dealing with applications for certain approvals, licenses or permits, but in practice these timelines are not always strictly followed.
[14] See Article 8 of the Security Assessment Measures.

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932
Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206
www.pillarlegalpc.com

	Standard Contract Approach	Professional Agency Certification Approach	Security Assessment Approach
Applicable Situations	The processor does not meet any of the following criteria (the "Threshold"): • The processor is a critical information infrastructure operator; • The processor processes personal information of more than one million individuals; • The processor provided personal information of more than 100,000 individuals to overseas recipients as of January 1 of the previous year; or • The processor provided sensitive personal information of more than 10,000 individuals to overseas recipients as of January 1 of the previous year.	This approach is an alternative for processors that does not meet the Threshold criteria, but: • process personal information within group companies under which personal information collected in China may be transferred to subsidiaries or affiliates in other parts of the world; or • process personal information from overseas but provides services to or analyzes behaviors of individuals located in China.	The processor meets any of the Threshold criteria.
Required Materials	• Standard contract; and • PIPIA report.	• Data processing agreement; • PIPIA report; and • Other materials, as necessary.	• Application form; • PIPIA report; • Data processing agreement between the processor and the overseas recipient; and • Other materials as required for a security assessment.
Requirements of a DPA[15]	The parties must use a standard contract provided by the CAC. The standard contract shall be signed on a "as is" basis. Any addition or revision to the standard contract shall not	No need to sign the standard contract provided by CAC, but the DPA put in place must include: • The basic information of the	No need to sign the standard contract provided by the CAC, but the DPA put in place must include: • The purpose, method and scope of data to be transferred;

[15] "DPA" here refers to any binding and enforceable legal documents between the personal information processor and overseas recipients that establish the rights and obligations of both parties in connection with cross-border transfer of personal information, including the standard contract provided by CAC and a data processing agreement between the parties.

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932
Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206
www.pillarlegalpc.com

	contradict with the terms and conditions already set forth therein.	personal information processor and the overseas recipient; • The purpose, category and scope of personal information to be transferred; • The security measures used to protect the rights and interests of personal information subjects; • A commitment from the overseas recipient to comply with unified personal information processing rules, the protection level of which cannot be lower than the standards stipulated in PIPL; • Agreement by the overseas recipient to accept supervision by the certification agency; • Acceptance of PRC laws as governing law by the overseas recipient; and • The information of the PRC entity responsible for any legal obligations or liabilities under applicable PRC data rules.	• The purpose and method of data processing activities by the overseas recipient; • The overseas storage location and retention period, as well as the measures to handle the data transferred overseas upon the expiration of the retention period, completion of the agreed purpose, or termination of the legal document; • Restrictions on transferring data to any other organization or individual by the overseas recipient; • The security measures to be adopted when there is any material change in the actual control or business scope of the overseas recipient, or when the data security protection policies, legislation, or cybersecurity environment change, or any other force majeure event occurs in the country or region where the overseas recipient is located which makes it difficult to ensure data security; • The remedial measures and liability for breach of contract and dispute resolution in the event of a breach of any data security protection obligation stipulated in the legal document; and

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932
Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206
www.pillarlegalpc.com

			• The requirements for proper emergency disposal and for ensuring the channels and ways for individuals to safeguard their personal information rights and interests when the data to be transferred is exposed to risks (e.g., tampering, damage, leakage, loss, relocation, or illegal use or acquisition.
Requirements of a PIPIA	The PIPIA must focus on the following matters: • The legality, legitimacy, and necessity of the personal information processing activities by the personal information processor and the overseas recipient in terms of the purpose, scope, method, etc.; • The quantity, scope, type, and sensitivity of personal information to be transferred overseas, and the risks that the cross-border transfer may pose to personal information rights and interests; • Whether the obligations undertaken by the overseas recipient and the management and technical measures and capabilities of the overseas recipient to perform such obligations can ensure the security of the data to be transferred;	The PIPIA must include as least the following two matters: • Whether the provision of personal information to overseas recipient is compliant with applicable laws and regulations; and • The impact on the rights and interests of personal information subjects, in particular with respect to certain legal protections and network security environments of the country or region where the overseas recipient is located.	The data cross-border security self-assessment shall focus on the following matters: • The legality, legitimacy, and necessity of the cross-border data transfer and the data processing by the overseas recipient in terms of the purpose, scope, method, etc.; • The quantity, scope, type, and sensitivity of the data to be transferred, and the risks that may be brought about by the cross-border data transfer to national security, public interests, or the lawful rights and interests of individuals or organizations; • Whether the obligations undertaken by the overseas recipient and the management and technical measures and capabilities of the overseas recipient to

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932
Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206
www.pillarlegalpc.com

	• The risk of disclosure, destruction, tampering, or misuse after the personal information is transferred overseas; • Whether there is a smooth channel for individuals to protect their personal information rights and interests; • The impact of personal information protection policies and regulations in the country or region of the overseas recipient on the performance of the standard contract; and • Other matters that may affect the security of personal information to be transferred overseas.		perform such obligations can ensure the security of the data to be transferred; • The risk of the data tampering, damage, leakage, loss, relocation or illegal use or acquisition during and after the cross-border data transfer; • Whether there is a smooth channel for individuals to safeguard their personal information rights and interests; • Whether data security protection obligations are sufficiently stipulated in the legal document with the oversea recipient; and • Other matters that may affect the security of a cross-border data transfer.
Procedures	Filing at a CAC local office within 10 working days after the effective date of the legal document.	Currently unclear.	• Submission of the required materials to a CAC local office; • Review by the CAC local office of the submitted documents, who will then pass such documents to the CAC; and • Material review by the CAC of the submitted documents the materials and disclosure to applicants of the result of such material review.

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932
Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206
www.pillarlegalpc.com