PILLAR LEGAL

Cross-Border Personal Information Processing Security Certification Specifications

CHINA REGULATION WATCH[1]

July 1, 2022

By: Zhu Ziwei | Alexandra Ashbrook

1. Introduction

On June 24, 2022, the Secretary of the National Information Security Standard Technology Committee (全国信息安全标准化技术委员会秘书处) issued Cross-Border Personal Information Processing Security Certification Specifications (个人信息跨境处理活动安全认证规范) ("Certification Specifications"), which provide practical guidance on professional agency certification approaches for companies that transfer personal information collected within the People's Republic of China ("China" or "PRC") to overseas recipients.

Pursuant to Article 38 of China's Personal Information Protection Law (个人信息保护法) ("PIPL"), before providing personal information to an overseas recipient, personal information processors[2] must either: (i) pass a security assessment conducted by the Cyberspace Administration of China (国家互联网信息办公室) ("CAC"), (ii) obtain a personal information protection certification from a professional agency in accordance with the regulations issued by the CAC; (iii) enter into a standard contract with the overseas recipient in a form provided by the CAC, or (iv) comply with other conditions prescribed by law, administrative regulations or the CAC. Currently, the above-mentioned approaches are not implementable, as the Personal Information Cross-Border Transfer Standard Contract Provisions (个人信息出境标准合同规定)[3] and the Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法)[4] are still in draft form and open for public comments. Although the Certification Specifications are now in effect, they were not issued by a legislative body or other department

【博申律師事務所】

[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] A personal information processor under PIPL plays a similar role as data controller under General Data Protection Regulations ("GDPR"). Pursuant to Article 73 of PIPL, personal information processor refers to any organization or individual that independently determines the purpose and method of processing activities.

[3] The draft Provisions on Personal Information Cross-Border Transfer Standard Contract were issued by CAC on June 30, 2022 (the "Standard Contract Provisions"), which (i) explains who is qualified to transfer personal information through standard contract approach; (ii) outlines filing requirements of standard contract approach, and (iii) provides a form of standard contract.

[4] The draft Cross-Border Data Transfer Security Assessment Measures were issued by CAC on October 29, 2021 (the "Security Assessment Measures"), which provides detailed instructions about (i) who is required to do security assessment, (ii) how to apply for security assessment, (iii) what's the standard of security assessment, and (iv) how long will the security assessment take.

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

with legislative power. In addition, these Certification Specifications do not provide information about which professional agencies are qualified to conduct the certification, nor how to apply for a certification. As a result, to ascertain the proper certification approach, more detailed regulations must first be issued by the CAC. Regardless, the Certification Specifications can serve as preparational guidance for covered companies.

2. Applicable Situations

Pursuant to the Certification Specifications, certification is a voluntary option recommended by the government, which is aimed to improve the efficiency of cross-border processing of personal information. It generally applies to the following two situations:

- Processing of 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. For these types of international companies, the company's PRC affiliates must receive certification and are furthermore responsible for any legal obligations and liabilities under applicable PRC data rules.

- Processing of personal information from overseas but providing services to or analyzing behaviors of individuals located in China, as specified in Article 3 of PIPL. Pursuant to Article 53 of PIPL, these overseas service providers must either establish an institution or appoint an agent in China to handle personal information protection matters, and moreover must file the contact information for any such institution or agent with the CAC. According to the Certification Specifications, any such institution or agent in China must receive certification and are responsible for any legal obligations and liabilities under applicable PRC data rules.

3. Requirements of Obtaining the Certification

Requirements for obtaining a personal information protection certification generally align with those under PIPL. However, the requirements as outlined in Section 4 of the Certification Specifications are more detailed. These certification requirements are summarized below.

Binding Agreement

Parties involved in cross-border data processing activities must enter into binding and enforceable legal documents (i.e., data processing agreements) to ensure that the rights and interests of the subjects of personal information receive protection. Such agreements should include:

- The personal information processor and overseas recipient's basic information;
- The category and scope of personal information being processed, as well as the purpose of processing such personal information;
- Security measures to protect 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;

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

- Agreement by the overseas recipient to accept supervision by the certification agency;[5]
- 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.

Personal Information Protection Officer and Department

The Certification Specifications also require both the personal information processor in China and the overseas recipient each appoint a personal information protection officer and establish an internal department that handles personal information protection matters. Such officer is required to have professional knowledge of personal information protection and relevant management experience, and furthermore must be a decision-making member of the company. Such internal department is responsible for (i) formulating and implementing a plan for the company's cross-border processing activities, (ii) conducting personal information protection impact assessments ("PIPIA"), (iii) supervising any cross-border processing activities, and (iv) receiving and handling requests and complaints from personal information subjects.

Personal Information Processing Rules

The personal information processor and overseas recipient must comply with unified personal information processing rules (usually in the form of a privacy policy), which shall include:

- The amount, scope, type and sensitivity of the personal information being processed;
- The purpose, method and scope of the processing activities;
- The retention period of personal information stored overseas, as well as the disposal methods after the retention period expires;
- The countries or regions where personal information will be stored;
- The resources and measures required to protect the rights and interests of personal information subjects;
- Compensation and remedies for personal information security incidents.

Personal Information Protection Impact Assessment

A PIPIA conducted for cross-border processing of personal information must address at least the following two matters:

- Whether the provision of personal information is compliant with applicable laws and regulations; and

[5] Neither the PIPL nor the Certification Specifications designate a certification agency or indicate how to qualify as a certification agency. According to Article 18 of Data Security Law (数据安全法), effective on September 1, 2021, the government will promote the development of data security testing, assessment, certification and other services, and provide supports to relevant professional agencies in conducting those data services in accordance with the law.

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 impact on the rights and interests of personal information subjects, in particular with respect to certain legal protections and network security environments of the destination country.

Other Obligations

Apart from the above, a few other obligations exist in connection with cross-border personal information processing certification. Some are the same as those required under PIPL, such as informing personal information subjects, obtaining separate consent prior to processing, and responding to the requests of those exercising personal information rights. Others are specific to receiving certification, such as suspending cross-border processing activities when it is difficult to ensure the security of personal information, as well as answering inquiries and accepting routine inspections by the certification agency.

4. Three Approaches to Cross-Border Provision of Personal Information

As noted above, cross-border provision of personal information is permissible under three approaches: (i) the CAC security assessment approach, (ii) the certification approach, and (iii) the standard contract approach. In light of the various documents and materials released by the relevant agencies thus far, using the standard contract is likely more convenient than the other two approaches. Using the standard contract only requires filing of the executed standard contract and associated PIPIA report at a CAC local office.[6] It does not appear the CAC will substantially review either of the submitted documents.

On the other hand, the security assessment approach requires significant effort to coordinate with the CAC and more time to complete. Apart from the data processing agreement and the PIPIA report, additional materials may also be requested for a more comprehensive assessment of the company's cross-border personal information processing activities. According to Article 40 of PIPL, the CAC security assessment will only apply to critical information infrastructure operators,[7] or personal information processors whose processing of personal information reaches the threshold amount prescribed by the CAC.[8]

[6] See Article 7 of the draft Standard Contract Provisions.

[7] Critical information infrastructure ("CII") refers to the key network facilities and information systems in important industries, which may seriously endanger the national security, national economy, people's livelihood and public welfare once they are subject to any destruction, loss of function or data leakage. Such industries include public telecommunication and information services, energy, transport, water conservancy, finance, public service, e-government and science and technology industries for national defense. See Article 2 of Regulations on the Security Protection of Critical Information Infrastructure (关键信息基础设施安全保护条例) issued by the State Council on July 30, 2021, and effective on September 1, 2021.

[8] Pursuant to Article 4 of the draft Security Assessment Measures, the thresholds that will trigger mandatory CAC security assessments refer to (i) processing personal information of more than one million individuals, or (ii) accumulatively provide personal information of more than 100,000 individuals to overseas recipients, or (iii) accumulatively provide sensitive personal information of more than 10,000 individuals to overseas recipients. The draft Standard Contract Provisions basically define the thresholds as the same, but it put a term to subsection (ii) and (iii), under which the accumulative amount will be calculated from January 1 of the previous year. That said, if the personal information provided to overseas recipient is under 100,000 or the sensitive personal information provided to overseas recipient is under 10,000 in 1-2 years, then CAC security assessment will not be required. To ascertain the threshold amount, we will need wait until the final version of the two regulations come out.

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

According to the Certification Specifications, the certification approach only applies to cross-border personal information processing activities of international companies or overseas service providers and is a voluntary option. That said, such international companies or overseas service providers are also typically qualified to simply use the standard contract so long as they do not meet the threshold amount promulgated by the CAC.

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