



PILLAR LEGAL

# Standard Contract for Cross-Border Transfers of Personal Information

[CHINA REGULATION WATCH](#)<sup>1</sup>

July 7, 2022

By: Zhu Ziwei | Alexandra Ashbrook

## 1. Introduction

On June 30, 2022, the Cyberspace Administration of China (国家互联网信息办公室)(“CAC”) released draft Personal Information Cross-Border Transfer Standard Contract Provisions (个人信息出境标准合同规定) (the “Draft Standard Contract Provisions”) together with the form standard contract (the “Standard Contract”) for public comments. Entering into a standard contract with overseas recipients of personal information in a form provided by the CAC is one of three approaches that enable personal information processors<sup>2</sup> to legitimately provide personal information collected in People’s Republic of China (“PRC” or “China”) to overseas recipients. The other two approaches include a security assessment by the CAC and receiving professional agency certification.<sup>3</sup> This article provides an overview of the Draft Standard Contract Provisions and an analysis of the Standard Contract.

## 2. Prerequisites of the Standard Contract Approach

Pursuant to Article 4 of the Draft Standard Contract Provisions, a personal information processor that meets all of the following conditions are qualified to provide personal information to overseas recipients by entering into a Standard Contract:

- The processor is not a critical information infrastructure operator;
- Personal information of less than one million individuals is processed;
- The processor did not provide personal information of more than 100,000 individuals to overseas recipients as of January 1 of the previous year; and
- The processor did not provide sensitive personal information of more than 10,000 individuals to overseas recipients as of January 1 of the previous year.

<sup>1</sup> 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](mailto:info@pillarlegalpc.com). Firm website: [www.pillarlegalpc.com](http://www.pillarlegalpc.com). © 2022 Pillar Legal, P.C.

<sup>2</sup> 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.

<sup>3</sup> See China Regulation Watch: [Cross-Border Personal Information Processing Security Certification Specifications](#) for more details.



Note that the standard contract approach is only designed for companies that send small portions of less sensitive personal information abroad. For companies that are involved in important industrial sectors, or cross the threshold amounts specified above, CAC requires such companies to pass a more comprehensive security assessment before any transfer of personal information out of China, as such transfer might impair the national security or public interests in China.<sup>4</sup>

### 3. Filing Requirement

Pursuant to Article 7 of the Draft Standard Contract Provisions, personal information processors must file the Standard Contract and associated personal information protection impact assessment (“PIPIA”) at a CAC local office within 10 working days after the effective date of the contract. Once the Standard Contract becomes effective, even before the Standard Contract is properly filed, companies may start the transfer of personal information out of China. It does not appear that that CAC will substantially review the submitted documents.

But according to Article 11 of the Draft Standard Contract Provisions, if CAC finds that the cross-border personal information processing activities no longer meet relevant requirements during the actual processing, personal information processors must immediately terminate the cross-border processing activities upon receipt of written notice from CAC. This seems to suggest that CAC may from time to time spot check the filed Standard Contract or may investigate a company when there is a complaint or report launched against the company.

Moreover, the parties may need to re-sign and refile the Standard Contract if any of the following conditions occur:

- There is any change to the purpose, scope, type, sensitivity, quantity, method, retention period, or storage location of personal information transferred overseas;
- There is any change to personal information protection policies and regulations in the country or region where the overseas recipient is located, which may affect personal information rights of the individuals; or
- Other circumstances occur that may affect personal information rights.

As a result, once there is any change in connection with the cross-border personal information processing activities, the parties shall not only inform the users (such as by updating a privacy policy), but also file a revised Standard Contract to keep the CAC updated. However, the rules are not clear about whether a new PIPIA should be conducted and relevant PIPIA report should be submitted. When actual implementation occurs, ideally regulators will provide different PIPIA options for different situations, such as waiver of a new PIPIA if only small changes in processing activities occur.

### 4. Content of the Standard Contract

<sup>4</sup> See Article 4 of the draft Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法) issued by CAC on October 29, 2021 for public comments.



All three approaches for cross-border transfer of personal information require the personal information processor and overseas recipient to enter into a binding agreement (i.e., a data processing agreement) that is sufficient to protect data security as well as the personal information rights of individuals. The draft Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法) outline several basic required agreement contents,<sup>5</sup> while 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) (the “Certification Specifications”) provide slightly more specific requirements.<sup>6</sup> Although the Standard Contract might be useful guidance on what the agreements will look like under the other two approaches, it is evident that the Standard Contract greatly limits the autonomy of the agreement, and intends to impose more obligations on both parties than as required by the other two approaches based on the currently issued rules.

### Limited Autonomy in Standard Contract

Although Standard Contract allows the parties to add additional clauses and terms in the agreement’s appendix, Section 9.1 of the Standard Contract indicates that in the event of any inconsistency between the Contract and any other existing agreement by and between the parties, the terms of Standard Contract shall prevail. In addition, Article 2 of the Draft Standard Contract Provisions also demand that other agreements entered into by and between the parties with respect to the cross-border transfer of personal information must not conflict with the Standard Contract. As a result, the obligations set forth in the main body of the Standard Contract cannot be adjusted.

Compared with the certification approach, the standard contract approach appears stricter in many aspects. For instance, the Certification Specifications require overseas recipients to accept the supervision of professional certification agencies, while the Standard Contract requires overseas recipients to accept the supervision of regulatory authorities. In addition, with respect to dispute resolution, the Standard Contract requires overseas recipients to settle lawsuits by individuals in a competent PRC court, and to settle any disputes between the signing parties in a competent PRC court or through arbitration taken in a country that is the participant of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. The Certification Specifications only require overseas recipient to accept PRC law as the agreement’s governing law and do not set any restrictions on dispute resolutions.

### Obligations of Overseas Recipients

---

<sup>5</sup> Pursuant to Article 9 of the draft Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法), the contract concluded between the domestic data processor and overseas recipient should include: (i) the purpose and method of cross-border data transfer, as well as the scope of data transferred; (ii) the place and period for storage of the data overseas, and the treatment measures for such data upon expiry of its storage period, completion of the agreed purpose or termination of the contract; (iii) provisions that restrict overseas recipient from further transferring the data to other organizations and individuals; (iv) the security measures to be adopted in the event that any material change occurs in the actual control or business scope of the overseas recipient, or that the legal environment of the country and region where the overseas recipient is located has changed so that it is difficult to safeguard data security; (v) the provisions that specify the liability for the breach of any data security protection obligation, as well as the provisions on dispute settlement, which shall be binding and enforceable; (vi) the emergency response measures to be adopted in case of any data leakage risk, and the smooth channel for individuals to safeguard the rights and interests in their personal information.

<sup>6</sup> See China Regulation Watch: [Cross-Border Personal Information Processing Security Certification Specifications](#) for more details.

The Standard Contract requires overseas recipients bear essentially all the obligations of a personal information processor under the Personal Information Protection Law (个人信息保护法) (“PIPL”). There are two points worth noting: one in connection with a company’s deletion and retention policy, another is related to a company’s data breach notification obligations.

Pursuant to Article 47 of PIPL, a personal information processor must delete the personal information of individuals if the personal information processor ceases to provide relevant services, or the retention period has expired. As a result, Section 3.4 of the Standard Contract requires overseas recipients to delete or anonymize personal information (including all backups) upon expiry of the storage period, unless a separate consent is obtained from the personal information subject regarding the storage period. Thus, once the personal information processor in China stops providing services in China, the overseas recipient must delete or anonymize any personal information collected in connection with the services as well unless such overseas recipient can obtain separate consent from users for any services it directly provided to users.

Pursuant to Article 57 of PIPL, if leakage of, tampering with, or loss of personal information occurs or may occur, a personal information processor must take immediate remedial measures and notify the authorities in charge of personal information protection and any individual affected. In Section 3.6 of the Standard Contract, in the event of a data breach, overseas recipients are not only required to inform the personal information processor of the incident, but also has the obligation to report the incident to the regulatory authorities of China. This requires overseas recipients be aware of the contact information and report mechanisms provided by PRC government authorities in order to timely report any incidents.

## 5. Confusion on Signing Entities

Unlike the Standard Contractual Clauses issued under GDPR, which provide four modules for different relationships between the data exporter and the data importer, China’s Standard Contract only has two roles: a personal information processor and an overseas recipient. This causes confusion around the signing parties of a Standard Contract in complicated data transfer contexts.

The current draft of the Standard Contract applies in situations where (i) a domestic personal information processor (“Domestic Controller”) transfers personal information to a foreign personal information processor (“Foreign Controller”), (ii) a Domestic Controller entrusts an overseas third party (“Foreign Processor”) to process personal information under its instruction and (iii) a Domestic Controller and a Foreign Controller jointly process personal information.

It is unclear whether a Standard Contract must be signed by a Domestic Controller or a domestic third party (“Domestic Processor”) with overseas recipients when a Domestic Controller entrusts a Domestic Processor to process personal information and the Domestic Processor further transfers personal information to its overseas affiliates for providing the services. Uncertainty also exists where a personal information processor outside of China processes personal information for providing services to, or analyzing behaviors of individuals



**PILLAR LEGAL**

located in China, as specified in Article 3 of PIPL. In such case, should the Standard Contract be signed by and between such foreign personal information processor and the relevant PRC agency or institution required by Article 53 of PIPL? In this scenario, the foreign personal information processor would be the overseas recipient under Standard Contract, but also a personal information processor according to PIPL. Thus, the foreign personal information processor's obligations under PIPL overlap with its obligations under the Standard Contract, convoluting the legal obligations of the designated PRC agency or institution.