GT GreenbergTraurig

Alert | Franchise & Distribution/Data, Privacy & Cybersecurity

March 2022

How Is International Franchising Affected by China's Personal Information and Data Compliance Regime?

This GT Alert covers the following:

- In 2021, China enacted Personal Information Protection Law and Data Security Law to regulate personal information and data processing activities. They both have extraterritorial application to overseas entities, including international franchisors.
- As a general rule, informed, voluntary, and express consent must be obtained before processing personal information. Separate consent must be obtained before processing activities with higher risks or impact on personal interest.
- Processors must take measures to ensure compliance with the laws in terms of outbound transfer of personal information, including the completion of personal information protection impact assessment, and government-led security assessment (if applicable).
- Before international franchisors receive personal information and data from Chinese outlets or franchisees, they should ensure the exporters' compliance with the laws, e.g., if the exporter has obtained informed consent from the individuals, completed personal information protection impact assessment, entered into data processing agreements with the recipients and filed for government-led security assessment (if applicable).

On Aug. 20, 2021, China promulgated the *Personal Information Protection Law* (*PIPL*), which took effect Nov. 1, 2021. Together, the *PIPL*, the *Cybersecurity Law* (which came into force June 1, 2017), and the *Data Security Law* (*DSL*, which came into force Sept. 1, 2021) form the fundamental legal framework that governs data security and processing of personal information (PI) and non-personal information (mainly the data other than PI) in mainland China.

The *PIPL* harmonizes the *Cybersecurity Law* and *DSL* by incorporating well-recognized data protection principles, including obtaining express and informed consent before collecting individuals' information; implementing a classified data protection system (with the introduction of enhanced protection for "sensitive personal information"); and setting a default rule for processors dealing with large amounts of PI they have collected or generated to store within China. Furthermore, the PIPL authorizes the Cyberspace Administration of China (CAC) to lead overall planning and coordination of PI protection and the relevant supervisory and regulatory work.

Territorial Scope of China's Personal Information and Data Compliance Regulations

The *PIPL* applies to all processing activities carried out in China. It has extraterritorial application to overseas processing of the PI of individuals located in China (where the purpose of such activities is to provide a product or service to such individuals), and to analyzing or assessing the behavior of individuals located in China (Article 3). The processors covered by the *PIPL's* extraterritorial application must establish a specialized agency or designate a representative in China to handle the matters related to the protection of PI; the name of such agency or the information (including the name and contact information) of such representative must be registered with the competent authorities in China (Article 53).

If an overseas organization or individual infringes the PI rights and interests of any Chinese citizen, or endangers the national security or public interests of China, the CAC may blacklist, restrict, or prohibit such overseas organization or individual from receiving the PI (Article 42).

Similarly, the *DSL* also has extraterritorial reach. It applies to data processing activities performed within the territory of China, as well as data processing activities performed outside of the territory of China that threaten national security, public interests, or the legitimate rights and interests of the citizens or organizations of China (Article 2).

PI and Enhanced Protection for Sensitive PI

The *PIPL* defines "sensitive personal information" as biometrics, religious beliefs, specific identities, medical and health, financial accounts, whereabouts and other information, as well as any PI of a minor under the age of 14 (Article 28). PI processors may process sensitive PI only with a specific purpose and sufficient necessity, and with strict protection measures taken including an advance impact assessment (the record of which must be kept for at least three years), record-keeping of processing activities, informing the individual of the necessity and impact on personal rights and interests, and a separate consent obtained from the individual (Articles 29, 30 and 56). Processors must formulate special rules for processing the PI of minors under 14 (Article 31).

Consent and Separate Consent

Under *PIPL* Article 14, where consent is required, individuals must voluntarily and expressly give their informed "consent." The *PIPL* provides exceptions where consent is not required, including where necessary to conclude or perform a contract (with the individual as a party), for certain human resource

management purposes, for performing legal duties or obligations, or for responding to a public health emergency or protection of life, etc. (Article 13).

Processors must obtain separate consent from individuals prior to information transfer, where the original PI processor transfers the PI it processed to other processors, and the individuals must be informed as to the details of other processors (including the name and contact information of the recipient, the purpose and method of processing, and the type of PI) (Article 23). Outbound transfers of PI additionally require the processor to inform the individuals of the methods and procedures for the individuals to exercise their rights under the *PIPL* against the overseas recipient (Article 39). Separate consent is also required for public disclosure of any PI processed by the processors (Article 25) and as mentioned above, for the processing of sensitive PI (Article 29).

Sharing PI with a Third Party

Depending on the status of a third-party recipient, *PIPL* distinguishes "transferring PI to other PI processors" from "entrusting a third party to process PI." In the former case, "other PI processors" may independently decide upon the purpose and method of PI processing; in the latter case, the entrusted third-party processes PI according to the agreed purpose, term, and method of processing agreed types of PI, among other rights and obligations, and must take agreed protective measures. As noted above, separate consent must be obtained prior to transferring PI to other PI processors, and the individuals must be informed of the basics of such other processors. In contrast, entrusting a third party to process PI does not require additional consent from the individuals, but the processor must supervise the processing activities by the entrusted party.

Cross-Border Transfer of PI

The *PIPL* permits cross-border (outbound in particular) transfer of PI required for business or other needs only if one of the following conditions is satisfied: (i) passing the CAC's security assessment, (ii) obtaining accreditation from the CAC-appointed professional agency, (iii) executing with the overseas recipient the CAC-approved standard agreements (which set out each party's respective rights and obligations, but which have not been officially released), or (iv) other conditions prescribed by the law and administrative regulations or set by the CAC. In addition, the PI processor must ensure the processing activities carried out by the overseas recipient meet the *PIPL*'s protection standards (Article 38).

Generally, PI collected and generated in China by critical information infrastructure operators or PI processors that process PI reaching certain volumes (as determined by the CAC) must be stored within China. If necessary to provide such information to an overseas recipient, passing the security assessment organized by the CAC will serve as a green light for the cross-border transfer of PI (Article 40). Pursuant to an October 2021 CAC draft governing data export (Measures for Security Assessment of Data Export, *Export Assessment Measures*), (1) providing important data to an overseas recipient or (2) providing PI of more than 100,000 individuals, or sensitive PI of more than 10,000 individuals, to an overseas recipient might also be subject to an additional security assessment organized by the CAC. The concept and scope of important data has not yet been formally defined.

All PI processors are required to complete an internal personal information protection impact assessment (PIPIA) before transferring PI outside of China (Article 55). The PIPIA should focus on three issues:

- If the purpose and method of the outbound transfer of PI is legal, justified, and necessary;
- The impact and security risk the outbound transfer of PI will have on personal interest;

- If the safeguard measures in place are legal, effective, and adequate for the risk levels.

In the *Export Assessment Measures*, the CAC enumerated considerations specifically relating to the PIPIA in the context of the outbound data transfer:

- Whether the purpose, scope, and means of an outbound transfer and data processing by the overseas recipient are legal, justified, and necessary;
- The volume, scope, types, and sensitivity of the data to be exported, and the potential risks to national security, public interest, and the legitimate interests of individuals;
- Whether the domestic transferring processor has implemented adequate management and technical measures to ensure data security;
- The risk of data leakage, loss, tampering, or abuse after the data transfer overseas, and whether there are open channels to personal information protection;
- Whether the data processing agreement with the foreign recipient clearly defines the responsibilities for data protection. (Article 5)

Impact on International Franchisor with Outlets in China

International franchise transactions often include bidirectional data transfers. Whether a franchisor and franchisee could be deemed a processor or an entrusted party of PI under Chinese laws and regulations depends largely on the method of collection and use of the PI. Although international franchisors are typically incorporated outside China, the jurisdictional scope of the *PIPL* and the *DSL*, and the prohibitive and restrictive measures taken by the CAC should not be ignored. For example, in many instances large, well-established franchisors receive customer information from franchisees and/or directly from customers in China through the use of mobile apps or franchisor websites. In such instances, those franchisors are more likely to be deemed a PI processor under the *PIPL*. However, at the moment, with certain exceptions in some franchise industries, the prevailing market practice for companies operating in China (not only in the context of franchising, but in almost all industries) when it comes to storing PI, is to store the PI within China.

Generally, international franchisors operate in China using one of two expansion models: (1) the franchisor establishes a wholly foreign-owned enterprise, WFOE, to either operate "company-owned" outlets or franchise within in China; or (2) the international franchisor grants third-party franchisees the right to operate one or more outlets in China. Oftentimes PI, such as customer contact information, expense records, shopping preferences, and other basic information of Chinese customers, is collected in China under both expansion models used by international franchisors and then is transmitted by either the WFOE or franchisees to the international franchisor's overseas headquarters for analyzing and global marketing. WFOEs and third-party franchisees that operate outlets in China and collect PI from customers would likely be considered a PI processor under the regulation of *PIPL*, and therefore both would be required to comply with the basic principles of processing PI and enhanced obligations regarding sensitive PI, which require the WFOE or third-party franchisee to obtain customer consent or separate customer consent, as applicable, as discussed above in this GT Alert.

Before an international franchisor receives any PI obtained from outlets operating in China, the franchisor should ensure the following conditions have been satisfied:

- The entity exporting PI (whether the WFOE or a third-party franchisee) must have obtained all required consent from, and have provided required notice to, the individuals whose PI was collected;
- The entity exporting PI (whether the WFOE or a third-party franchisee) must have completed the PIPIA;
- The entity exporting PI (whether the WFOE or a third-party franchisee) should have entered into a data processing agreement with the foreign recipient (most likely either the international franchisor entity or a data center) according to the standard agreements approved by the CAC; and
- The outbound transfer of PI must also have passed an additional security assessment as required by the CAC in instances where the amount of PI and sensitive PI to be exported from customers of outlets operating in China reaches more than 100,000 individuals, with respect to PI, or 10,000 individuals, with respect to sensitive PI. In such instances the entity exporting PI should communicate with the CAC to confirm whether an additional security assessment is necessary.

Further, whenever international franchisors receive PI from individuals in China, in addition to contractually requiring third-party franchisees to comply with applicable privacy laws in China, the international franchisor should regularly audit the PI collection, and consent and notification practices of its WFOE or third franchisee(s) for compliance with the *PIPL* and the *DSL*.

International franchisors will need to further evaluate the collection and exporting of PI overseas from China after the CAC officially releases the identification rules of important data. Nonetheless, international franchisors should consider tailoring their PI and data collection practices to fit their specific needs, and take such needs into consideration when negotiating international franchise agreements for new markets, such as China.

Authors

This GT Alert was prepared by:

- Alan R. Greenfield | +1 312.456.6586 | greenfieldalan@gtlaw.com
- George Qi | +86 (0) 21.6391.6633 | qig@gtlaw.com
- Dawn (Dan) Zhang | +86 (0) 21.6391.6633 | zhangd@gtlaw.com
- John Gao | +86 (0) 21.6391.6633 | gaoj@gtlaw.com