GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

September 2021

China Promulgates Personal Information Protection Law

On Aug. 20, 2021, after two rounds of public comments on China's draft *Personal Information Protection Law* (*PIPL*),[1] China promulgated the final version of the *PIPL*, which takes effect Nov. 1, 2021. Together, the *PIPL*, *Cybersecurity Law* (which came into force June 1, 2017) and *Data Security Law* (which came into force Sept. 1, 2021) now form the fundamental legal framework that governs data security and processing of personal information (PI) and non-personal information. The *PIPL* harmonizes the *Cybersecurity Law* and *Data Security Law*[2] by incorporating well-recognized data protection principles, including obtaining express and informed consent before collecting the individuals' information; implementing a classified data protection system (with the introduction of enhanced protection for "sensitive personal information"); and setting a default rule for the "critical information infrastructure operators" (CIIOs) and processors dealing with large amounts of PI they have collected or generated to store within China. 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. This GT Alert summarizes the *PIPL*.

1 *See* January 2021 GT Alert, China Releases Draft Personal Information Protection Law.
2 *See* July 2021 GT Alert, China Finalizes Data Security Law.

Territorial Scope of the *PIPL*

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

If the PI rights and interests of any citizen of China are infringed, or the national security or public interests of China are endangered by any overseas organization or individual, the CAC may take measures against such overseas organization or individual, including blacklisting, restricting, or prohibiting such overseas organization or individual from receiving the PI (Article 42).

The *PIPL* adopts a similar approach as that of the *Data Security Law*, by introducing reciprocal measures against any country or region that takes any discriminatory prohibition, restriction, or any other measures against China. However, the *Data Security Law* limits the applicable scope of such discriminatory measures to data and data development and use technology, while the *PIPL* sets the relevancy to PI protection (Article 43).

PI and Enhanced Protection for Sensitive PI

Excluding information that has been anonymized, "personal information" under the *PIPL* refers to any kind of information related to an identified or identifiable natural person, recorded electronically or otherwise. "Processing" includes the collection, storage, use, transmission, provision, disclosure, and deletion of PI (Article 4). PI processing activities must follow the basic principles of lawfulness, legitimacy, necessity, and good faith (without misleading, fraud, or coercion); openness and transparency (with the rules, purpose, method and scope of processing activities disclosed); direct and specific relevance; minimum impact on personal rights and interests; minimum necessary scope of collection; quality assurance (avoiding inaccuracy and incompleteness; and prohibition against illegality (prohibiting illegal sale, provision, or publication; and prohibiting activities endangering national security and public interest) (Articles 5, 6, 7, 8 and 10).

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 the in-advance impact assessment (the record for which must be kept for at least three years), record-keeping of the 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). Special rules must be formulated by processors for processing the PI of minors under the age of 14 (Article 31).

Consent and Separate Consent

Informed "consent" as the general legal basis for processing of PI must be made by individuals voluntarily and expressly (Article 14). The *PIPL* provides exceptions where consent is not required, including where necessary to conclude or perform a contract (with the individual as a party), necessary for certain human resource management purposes, necessary for performing legal duties or obligations, or necessary for responding to a public health emergency or protection of life, etc. (Article 13).

Separate consent must be obtained 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 the public disclosure of any PI processed by the processors (Article 25) and as mentioned above, for the processing of sensitive PI (Article 29).

In response to the specific privacy challenges brought by the mass adoption of surveillance cameras and artificial intelligence in modern cities in China, the *PIPL* requires any image capturing or personal identification equipment installed in a public place to be necessary to maintain public security, and with prominent reminders visible. The personal images and identification information collected from the equipment may only be used to maintain public security, except when separate consent is obtained from individuals (Article 26).

Automated Decision-Making

The *PIPL* defines "automated decision-making" as analysis or assessment as well as automatic decision-making of personal behavior and habits, interests and hobbies, financial, health or credit status or other information through a computer program (Article 73). The processors using PI for automated decision-making must ensure the transparency of the decision-making and fairness and impartiality of the results, and the automated decision-making must not be used to impose unreasonable differential treatment on individuals in terms of transaction prices and other transaction conditions. If the automated decision-making is used for commercial marketing or information pushing to individuals, processors must provide individuals with options that are not based on the individuals' personal characteristics, or convenient methods for the individuals to refuse such commercial marketing or information pushing. In addition, the *PIPL* allows individuals to have the right to request processors to give explanations or refuse to accept the processors making decisions solely based on automated decision-making, if such decisions have a major impact on the individuals' rights and interests. (Article 24).

Designation of Data Protection Officer

The *PIPL* requires the designation of a data protection officer (DPO) as the responsible person to supervise PI processing activities and protection measures taken by certain processors, i.e., those processing PI at a volume that exceeds the threshold to be specified by the CAC. The contact information of the DPO must be disclosed to the public, and the details of the DPO (including name and contact information) must be registered with the relevant authorities (Article 52).

Stricter Requirements on Critical Internet Platform Service Providers

Faced with technology innovation and significant growth of tech giants in China, the *PIPL* imposes stricter requirements on the critical internet platform service providers that have a large user base and operate complex types of business. Such internet platform service providers must (i) establish a comprehensive PI-protection compliance policy and system, and form an independent supervision team mainly composed of external members, (ii) formulate platform rules to specify the standards for PI processing and the obligations of PI protection, by following the principles of openness, fairness, and impartiality, (iii) cease to provide the service to those in-platform product or service providers that seriously violate the applicable laws or administrative regulations in processing PI, (iv) regularly publish a report on the social responsibility for PI protection, and accept public supervision (Article 58).

Cross-Border Transfer of PI

The cross-border (outbound in particular) transfer of PI required for business or other needs is permitted under the *PIPL* only if one of the following conditions is satisfied: (i) passing the security assessment organized by the CAC, (ii) obtaining the accreditation from the professional agency appointed by the CAC, (iii) executing with the overseas recipient the standard agreements approved by the CAC (which set out each party's respective rights and obligations), (iv) any 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, the PI collected and generated in China by the CIIOs or the PI processors that process PI reaching certain volumes (as determined by the CAC), must be stored within China. If it is 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). The same rule applies to the PI processed by the national authorities (which in general must be stored in China) – the CAC's security assessment organized must be passed prior to the necessary outbound provision or transfer of the PI processed by the national authorities (Article 36).

The *PIPL* adopts a similar restriction as the *Data Security Law* for outbound data transfer upon requests of foreign judicial or law enforcement authorities, except the *PIPL* governs PI while the *Data Security Law* applies to all data (no matter if recorded in electronic or other form). Chinese authorities will handle the requests from overseas judicial or law enforcement authorities for provision of PI stored in China in accordance with applicable international treaties or agreements, or in accordance with the principles of equality and reciprocity. Without approval from the competent authorities, PI processors may not provide any PI stored in China to a foreign judicial or law enforcement authority (Article 41).

Legal Liabilities for *PIPL* Violations

Breach of the *PIPL* can result in three kinds of legal liability – administrative, civil, and criminal.

Administrative liability. The responsible processor may have to relinquish the illegal gains, and may be fined up to 50 million Chinese yuan or 5% of the prior year's annual revenue (whether the revenue refers to the global revenue or only the revenue generated in China is to be specified). The non-monetary administrative penalties include rectification orders, warnings, suspension or cessation of services, cessation of operations or revocation of permits or business licenses, and recording such violation into the credit file and disclosure to the public. In addition, the person in charge or other directly liable individual may be fined up to 1 million Chinese yuan, and prohibited from acting as a director, supervisor, senior officer or DPO at the relevant company (Article 66).

Civil liability. The responsible processor will bear the tort liability (including compensation for damages), if the rights and interests of PI are damaged by the processing activities. The *PIPL* introduces a presumption of liability on the processor, and the burden of proof will be borne by the processor (Article 69). This emphasizes the importance of processors keeping proper records and evidence to prove the lawfulness and appropriateness of their activities. If the rights and interests of many individuals are infringed by a processor in violation of the *PIPL*, the prosecutors, consumer organizations, and organizations designated by the CAC may take legal action against the processor (Article 70).

Criminal liability. The *PIPL* refers to the Chinese criminal code to pursue criminal liability of the responsible parties (Article 71).

GT GreenbergTraurig

Authors

This GT Alert was prepared by:

- George Qi | +86 (0) 21.6391.6633 | qig@gtlaw.com
- Qianqian Li | +86 (0) 21.6391.6633 | liq@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.