GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

January 2021

China Releases Draft Personal Information Protection Law

On Oct. 21, 2020, China published a draft of the Personal Information Protection Law (*Draft*) with a month-long public comment period. Once promulgated, the Personal Information Protection Law, along with the Cybersecurity Law and the Data Security Law, will be the three fundamental data protection laws in China. No information has been provided as to a timeline for a revised or final version of the *Draft*.

Scope of the Draft's Application

According to Article 4 of the *Draft*, personal information (PI) refers to "all kinds of information" related to identified or identifiable natural persons as recorded by electronic or other means, but excluding information after anonymization (the process of handling PI to de-identify a specific natural person and making its original status non-restorable). The handling of PI includes collection, storage, use, processing, transmission, provision, disclosure and other activities. The *Draft* refers to organizations and individuals handling the activities as "personal information handlers" (PIH) which autonomously determine the handling purpose, method, or any other related matter, and which are required by Article 9 to adopt safeguards necessary to secure the PI they handle.

The *Draft* language protects the PI of natural persons and applies to:

a. the activities conducted in China mainland by organizations and individuals which handle the PI, and

b. the activities conducted by organizations located outside of mainland China who handle the PI of natural persons physically in mainland China where such handling serves the purpose of (i) providing products or services for natural persons in mainland China, (ii) analyzing and evaluating the behaviors of natural persons in mainland China, or (iii) other circumstances as stipulated by laws and administrative regulations.

Per Article 52, for PIHs whose activities are conducted outside mainland China, a specialized entity must be set up or a representative appointed in mainland China to handle the matters concerning PI protection, providing the name and contact information of such entity or individual to the PI protecting government agencies.

Consent and Right to Be Informed

The *Draft* allows the handling of PI without consent under certain circumstances, where (i) within the public interest within reasonable scope, such as for news reporting, or (ii) it is essential for (a) entering into or performing a contract with the person, or (b) performing statutory responsibilities or obligations, or (c) responding to public health incidents or for protecting the life, health, or property safety of natural persons in emergency situations, or (iii) other circumstances as stipulated by laws and administrative regulations.

Under Article 17, no PIH can refuse to provide products or services because an individual does not give consent to the handling, or withdraws consent, except if the PI is essential for the provision of such products or services. Consent must be obtained from the individual voluntarily and explicitly, with his/her full knowledge of such PI handling (including the identity and contact information of PIH, purpose and method of such handling, type and storage period of personal information to be handled, ways and procedures for the individuals to exercise their rights under the *Draft*, and other matters that must be communicated in accordance with laws and administrative regulations).

If the handling involves sensitive PI, the PIH must state the necessity of handling such information and the impact on the relevant individual. Under the Draft, "sensitive personal information" refers to the information (including race, nationality, religious belief, personal biological features, medical history, health) which, once leaked or illegally used, may lead to personal discrimination or serious harm to personal and property safety. The *Draft*, while similar to Europe's GDPR in its heightened protections for sensitive PI, is potentially even broader in some regards – as it includes within its definition financial account information and individuals' location – but narrower in others, such as by excluding trade union membership, political opinions, genetic and biometric data, and sexual life-related information from the definition. Separate consent from the individual must be obtained for sensitive PI.

Under the *Draft*, installation of image collection and personal identity recognition devices in public areas can only be used for public security, and with clear signage. Such PI can only be used for safeguarding public security and cannot be disclosed to the public or any third party, unless the organization collecting the PI obtains the individual's separate consent or laws or regulations permit such use or sharing.

The consent from the guardian of a minor must be obtained if the PIH knows or should know that the PI belongs to a minor under the age of 14, aligning with children's privacy laws in the United States.

Any change to the PI-handling purpose, method, or type requires separate consent. In case of transfer of PI due to merger, split or other reasons, the PIH must inform the individuals of the identity and contact information of the recipient party, with the recipient party bearing the responsibilities as a PIH. Separate

consent still needs to be obtained if the original purpose or method of handling is changed by the recipient party.

If the PIH provides PI to a third party (i.e., a "recipient" or "entrusted party") after its handling, the PIH must inform the individuals of the third party's identity, contact information, handling purpose, handling method, and types of PI, and additionally obtain the specific consent from the individual for such provision. The third party must, within the above scope of handling purpose, method, and types, handle such PI. Any change to the handling purpose or method requires the individual's consent. If the PIH provides anonymized information to a third party, the third party may not use technical means to re-identify the individuals.

Other Rights

Along with the right to consent to handling their PI, individuals also have the right to (a) withdraw consent from the PIH, (b) access and copy their PI from the PIH, (c) request that the PIH rectify or make the PI complete, (d) deletion of the PI (where the agreed retention period has expired; the handling purpose has been achieved; the PIH ceases to provide products or services; consent from the individual has been withdrawn; the handling by PIH violates laws, administrative regulations, the agreement reached about the handling; or other circumstances as specified by laws and regulations), (e) request that the PIH explain the rules on its PI handling. To respond to the above rights, the PIH must establish a mechanism for processing the individuals' requests, and such mechanism must include the explanation of reasons for its decline of the request.

Also, to the extent an organization uses automated decision-making, pursuant to Article 25 the individual has the right to (a) an explanation from the PIH on whether the automated decision-making has a material impact on the individual's rights and interests, and (b) refuse allowing the PIH to make decisions that rely only on automated decision-making. The PIH must ensure the transparency of such automated decision-making, and the fairness and reasonability of the results. When it conducts marketing and push notifications via automated decision-making, the PIH must provide options for either (without targeting an individual's personal characteristics) with the automated decision-making option for the individuals.

Other PIH Obligations

In addition to establishing the above-listed mechanisms, the PIH must also:

- develop internal management systems and operating procedures;
- implement hierarchical and categorized PI management;
- take appropriate security technical measures such as encryption and de-identification;
- reasonably determine the operating permission for PI handling, and conduct regular security education and training for its employees;
- develop and organize the implementation of emergency plans for PI security incidents, and carry out other measures prescribed by laws and regulations.

Cross-Border Transfer and Responsibilities by PIH Outside the Mainland

Pursuant to Article 38, if the PIH handles PI outside mainland China for business needs (which excludes the cross-border transfer of PI for non-business uses, e.g., to provide information to family members abroad), the PIH must meet one of the following conditions: (a) it must pass a security assessment

organized by the national cyberspace authorities in accordance with the *Draft* (under Article 40 of which, critical information infrastructure operators and the PIH (which handles the personal information up to an amount as specified by the national cyberspace authorities) shall store the PI collected and generated from the mainland within the mainland, while the security assessment organized by the national cyberspace authorities shall be conducted and passed if necessary to provide such information outside the mainland, unless otherwise specified by the laws and regulations); or (b) it must have undertaken PI protection certification conducted by professional agencies; or (c) it must have signed a contract with the overseas receiving parties which provides the rights and obligations of both parties, and supervising their activities of handling PI to ensure the relevant standards under the *Draft* are met; or (d) it must meet other conditions stipulated by laws, administrative regulations, or the national cyberspace authorities. The *Draft*, unlike the GDPR, does not contain provisions for adequacy determinations in third countries.

In 2019, the relevant authority – the Cyberspace Administration of China – released a document for the above security assessment for cross-border transfers of PI, calling for public comments on the *Circular of the Cyberspace Administration of China on Seeking Public Opinions on the Measures for Security Assessment for Cross-border Transfer of Personal Information*. This draft specifies that multiple assessments (for the provision of PI to one recipient on multiple occasions or continuously) are not required, while a new security assessment is required every two years or when the purpose, type, or overseas retention period related to the cross-border transfer of PI changes. In contrast, separate security assessments must be declared for the provision of PI to different recipients.

A risk assessment shall be conducted (unlike the above security assessment) where it is truly necessary for the national authorities to provide PI to entities outside of the mainland. The risk assessment shall include: (a) whether the PI-handling purpose and method are legitimate, proper, and necessary, (b) the impact on the individual and the risk level, and (c) whether the security protection measures taken are legitimate, effective, and commensurate with the risk level. Such risk assessment reports and handling status records shall be preserved for at least three years. An in-advance risk assessment shall also be conducted for handling sensitive PI, using PI for automated decision-making, entrusting any other person with handling, providing, or disclosing PI to any third party, providing PI to outside of the mainland, and other handling activities with a significant impact on individuals.

The PIH must inform the individual of the provision of PI to outside the mainland (stating the identity and contact information of the receiving party, the handling purpose and method, the type of PI to be handled by the receiving party, as well as the way by which the individuals can exercise rights over the receiving party under the *Draft*). Separate consent from the individuals must be obtained. Article 40 of the *Draft* maintains prior versions' data localization requirements for PHI "handling [PI] reaching quantities provided by the State cybersecurity and informatization department," but this quantity has not yet been specified.

Fines for Violations of the *Draft*

Article 59 of the *Draft* provides regulators broad powers to investigate potential violations of PI rights, including power to question employees, conduct on-site investigations, inspect business records, and seize equipment.

Violations of the *Draft* will result in an administrative order for rectification, confiscation of the unlawful income, and a fine up to 1 million Yuan imposed on the PIH, and a fine between 10,000 and 100,000 Yuan imposed on the directly liable person-in-charge or any other directly liable individual. In severe cases, the fine imposed on the PIH will be increased in an amount up to 50 million Yuan or 5% of last year's annual revenue. In addition to the fines, a business could have its operations in China suspended

and/or reported to relevant authorities for the cancellation of the related business permit, and the business employees responsible for compliance can be found personally liable and fined along with any other directly liable individual, up to 1 million Yuan. In addition, such violations will be recorded in the credit files and disclosed to the public.

** This GT Alert is limited to non-U.S. matters and law.*

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
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Darren Abernethy | +1 415.655.1261 | abernethyd@gtlaw.com