SQUIRE PATTON BOGGS

China's Personal Information Protection Law

Asia Pacific – 27 August 2021

After three rounds of revisions, on August 20, 2021, the National People's Congress Standing Committee of the People's Republic of China officially passed the Personal Information Protection Law (the PIPL).

- **Fundamental principle** – The fundamental principle under the PIPL is that collection and processing of personal information ("PI") should be limited only to the minimum level as necessary to fulfill the specific purpose of PI processing; or the so-called "as minimum and as necessary" principle. PI processing beyond the minimum and the necessity levels may be found as being a violation of the PIPL, even if individual consent is obtained or other formality is fulfilled. A PI processing and compliance program should always be set up with the fundamental principles in mind.
- **Effective date** – Although a number of important provisions will require clarification through implementing rules by regulatory authorities, the PIPL will take effect on **November 1, 2021**, without the over-six-month grace period as previously expected. Companies doing business in China or otherwise processing Chinese residents' data need to take immediate actions to comply with the PIPL. (Note: the PIPL applies only in Mainland China. Hong Kong has its own data protection rules, which are not affected).
- **Extra-territorial effect** – For the first time, the PIPL will apply to the processing of Chinese residents' data outside of China if it is to provide goods or services to people within China, to analyze the activities of persons within China, or as otherwise proscribed by law. Currently, personal data-related Chinese laws do not apply to processing activities outside of China, for example, where the collecting entities and the servers hosting the data are located outside of China. Such activities will now be bound by the PIPL and the relevant entities should particularly note the specific consent requirement and the data localization requirements under the PIPL.
- **Legal bases for processing** – In the following situations, processing of PI is permitted by law without obtaining consent from the data subject:
  - For the performance of a contract with the individual or for purpose of human resources management according to legally adopted labor policies
  - Where it is necessary to perform statutory duties
  - A few other situations, such as where it is necessary for the protection of life, health and property, news reporting, or as otherwise required by law

  "For the purpose of human resources management according to legally adopted labor policies" has been newly added in the final PIPL version, which is likely to facilitate employee data management. It makes room for companies to rely on its legally adopted employment policies, such as its employee handbook, to process employees' PI, instead of obtaining consent from each individual employee.
- **Data localization requirements** – Critical Infrastructure Information (CII) operators or entities processing a large amount of personal information must store personal information within the territory of Mainland China. If they need to transfer such personal information to points outside China, the transfer must pass a security assessment administered by the government authorities.

  Critical Information Infrastructure (CII) refers to the network and IT system that are critical to national security and public interest, such as government system, utilities, financial system, public health, etc. Operators of CII are subject to much stricter rules in terms of data security and cross-border data transfer. Every company operating in China should conduct a self-assessment as to whether it might be deemed as a CII operator.

  "A large amount of personal information" is not defined in the PIPL. A few other data-related regulations or draft regulations, which define "large amount" as 500,000 or 1 million individuals, may shed some light on the threshold. It is expected to be clarified by the authorities.
- **Cross-border transfer** – Other than a CII operator and a large volume of PI as mentioned above, a cross-border transfer is only allowed if the PI processor meets one of the following requirements:
  - It passes a security assessment organized by the Cybersecurity Administration of China (CAC).
  - It is certified by a specialized agency for the protection of PI by CAC.
  - It enters into a contract with the overseas recipient under the standard contract formulated by the Cyberspace Administration of China, the form of which has not yet been published.

- **Separate consent** – The PIPL requires the PI processor to obtain "separate consent" in various occasions, including cross-border transfer, sharing or entrusting PI to a third party and processing of sensitive PI. "Separate consent" means the consent should be specifically relating to the relevant purpose, and not be bundled into a privacy policy covering multiple processing activities. For each such separate consent, certain information must be disclosed to the data subject as provided under the PIPL.
- **Penalties** – Violations of the law with serious consequences may be penalized up to 5% of the prior year's turnover, and/or the ceasing of services, including the possible revocation of the business license.

We will provide a more in-depth summary of the PIPL shortly.

Contacts

Lindsay Zhu
Partner, Shanghai
T +86 21 6103 6303
E lindsay.zhu@squirepb.com

Scott Warren
Partner, Tokyo
T +81 3 5774 1813
E scott.warren@squirepb.com

About Us

Our China team works closely with our Data Privacy, Cybersecurity & Digital Assets team, which has more than 20 years of experience in data protection. We cover the full scope of privacy and cyber services, including proactive compliance work and risk assessments, incident preparation and response, post-incident remediation and crisis management, as well as privacy and cybersecurity litigation strategy. We also work with local firms to engage with local regulators and defend our clients.