GIBSON DUNN

September 10, 2021

# CHINA PASSES THE PERSONAL INFORMATION PROTECTION LAW, TO TAKE EFFECT ON NOVEMBER 1

To Our Clients and Friends:

On August 20, 2021, the Standing Committee of China's National People's Congress passed the Personal Information Protection Law ("PIPL"), which will take effect on November 1, 2021. We previously reported on this development here, when the law was in draft form. An unofficial translation of the newly enacted PIPL is available here and the Mandarin version of the PIPL is available here.[1]

The PIPL applies to "personal information processing entities ("PIPEs")," defined as "an organisation or individual that independently determines the purposes and means for processing of personal information." (*Article 73*). The PIPL defines "personal information" broadly as "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person," excluding anonymized information, and defines "processing" as "the collection, storage, use, refining, transmission, provision, public disclosure or deletion of personal information." (*Article 4*).

The PIPL shares many similarities with the EU's General Data Protection Regulation (the "GDPR"), including its extraterritorial reach, restrictions on data transfer, compliance obligations and sanctions for non-compliance, amongst others. The PIPL raises some concerns for companies that conduct business in China, even where such companies' data processing activities take place outside of China, and the consequences for failing to comply could potentially include monetary penalties and companies being placed on a government blacklist.

Below, we describe the companies subject to the PIPL, key features of the PIPL, and highlight critical issues for companies operating in China in light of this important legislative development.

## I. Which Companies are Subject to PIPL?

- ***The PIPL applies to cross-border transmission of personal information and applies extraterritorially***. Where PIPEs transmit personal information to entities outside China, they must inform the data subjects of the transfer, obtain their specific consent to the transfer, and ensure that the data recipients satisfy standards of personal information protection similar to those in the PIPL.The PIPL applies to organisations operating in China, as well as to foreign organisations and individuals processing personal information outside China in any one of the following circumstances: (1) the organisation collects and processes personal data for the purpose of providing products or services to natural persons in China; (2) the data will be used in analysing and evaluating the behaviour of natural persons in China; or (3) under other unspecified "circumstances stipulated by laws and administrative regulations" (*Article 3*). This is an important similarity between the PIPL and GDPR, as the GDPR's data protection obligations apply to non-EU data controllers and processors that track, analyze and handle data from visitors within the EU. Similarly, under the PIPL, a foreign receiving party must comply

with the PIPL's standard of personal information protection if it handles personal information from natural persons located in China.

- ***The PIPL gives the Chinese government broad authority in processing personal information***. State organisations may process personal information to fulfil statutory duties, but may not process the data in a way that exceeds the scope necessary to fulfil these statutory duties (*Article 34*). Personal information processed by state organisations must be stored within China (*Article 36*).

**II. Key Features of PIPL**

- ***The PIPL establishes guiding principles on protection of personal information***. According to the PIPL, processing of personal information should have a "clear and reasonable purpose" and should be directly related to that purpose (*Article 6*). The PIPL requires that the collection of personal information be minimized and not excessive (*Article 6*), and requires PIPEs to ensure the security of personal information (*Articles 8-9)*. To that end, the PIPL imposes a number of compliance obligations on PIPEs, including requiring PIPEs to establish policies and procedures on personal information protection, implement technological solutions to ensure data security, and carry out risk assessments prior to engaging in certain processing activities (*Articles 51 – 59*).

- ***The PIPL adopts a risk-based approach, imposing heightened compliance obligations in specified high-risk scenarios.*** For instance, PIPEs whose processing volume exceeds a yet-to-be-specified threshold must designate a personal information protection officer responsible for supervising the processing of personal data (*Article 52*). PIPEs operating "internet platforms" that have a "very large" number of users must engage an external, independent entity to monitor compliance with personal information protection obligations, and regularly publish "social responsibility reports" on the status of their personal information protection efforts (*Article 58*).The law mandates additional protections for "sensitive personal information," broadly defined as personal information that, once disclosed or used in an illegal manner, could infringe on the personal dignity of natural persons or harm persons or property (*Article 28*). "Sensitive personal information" includes biometrics, religious information, special status, medical information, financial account, location information, and personal information of minors under the age of 14 (*Article 28*). When processing "sensitive personal information," according to the PIPL, PIPEs must only use information necessary to achieve the specified purpose of the collection, adopt strict protective measures, and obtain the data subjects' specific consent (*Article 28-29*).

- ***The PIPL creates legal rights for data subjects.*** According to the new law, PIPEs may process personal information only after obtaining fully informed consent in a voluntary and explicit statement, although the law does not provide additional details regarding the required format of this consent. The law also sets forth certain situations where obtaining consent is unnecessary, including where necessary to fulfil statutory duties and responsibilities or statutory obligations, or when handling personal information within a reasonable scope to implement news reporting,

public opinion supervision and other such activities for the public interest (*Articles 13-14, 17*). Where consent is required, PIPEs should obtain a new consent where it changes the purpose or method of personal information processing after the initial collection (*Article 14*). The law also requires PIPEs to provide a convenient way for individuals to withdraw their consent (*Article 15*), and mandates that PIPEs keep the personal information only for the shortest period of time necessary to achieve the original purpose of the collection (*Article 19*).If PIPEs use computer algorithms to engage in "automated decision making" based on individuals' data, the PIPEs are required to be transparent and fair in the decision making, and are prohibited from using automated decision making to engaging in "unreasonably discriminatory" pricing practices (*Article 24, 73*). "Automated decision-making" is defined as the activity of using computer programs to automatically analyze or assess personal behaviours, habits, interests, or hobbies, or financial, health, credit, or other status, and make decisions based thereupon (*Article 73(2)*).When individuals' rights are significantly impacted by PIPEs' automated decision making, individuals can demand PIPEs to explain the decision making and decline automated decision making (*Article 24).*

**III. Potential Issues for Companies Operating in China**

The passage of the PIPL and the uncertainty surrounding many aspects of the law creates a number of potential issues and concerns for companies operating in China. These include the following:

- ***Foreign organisations may be subject to the PIPL's regulatory requirements***. The PIPL applies to data processing activities, even where those activities take place outside of China, provided they are carried out for the purpose of conducting business in China or evaluating individuals' behavior in the country. The law is currently silent on how close the nexus must be between the data processing and Chinese business activities. The law also mandates that data processing activities taking place outside of China are subject to the PIPL under "other circumstances stipulated by laws and administrative regulations." At present there is no guidance as to what these circumstances will be.Foreign organisations subject to the PIPL will need to comply with requirements including security assessments, assigning local representatives to oversee data processing, and reporting to supervisory agencies in China, though the exact parameters of these requirements remain unclear (*Articles 51–58*).

- ***The PIPL creates penalties for organisations that fail to fulfil their obligations to protect personal information* (*Article 66*)**. These penalties include disgorgement of profits and provisional suspension or termination of electronic applications used by PIPEs to conduct the unlawful collection or processing. Companies and individuals may be subject to a fine of not more than 1 million RMB (approximately $154,378.20) where they fail to remediate conduct found to be in violation of the PIPL, with responsible individuals subject to fines of 10,000 to 100,000 RMB (approximately $1,543.81 to $15,438.05).Companies and responsible individuals face particularly stringent penalties where the violations are "grave," a term left undefined in the statute. In these cases, the PIPL allows for fines of up to 50 million RMB (approximately $7,719,027.00) or 5% of annual revenue, although the PIPL does not specify which parameter serves as the upper limit for the fines. Authorities may also suspend the offending business

activities, stop all business activities entirely, or cancel all administrative or business licenses. Individuals responsible for "grave" violations may be fined between 100,000 and 1 million RMB (approximately $15,438.29 to $154,382.93), and may also be prohibited from holding certain job titles, including Director, Supervisor, high-level Manager or Personal Information Protection Officer, for a period of time. In contrast, fines for severe violations of the GDPR can be up to €20 million (approximately $23,486,300.00) or up to 4% of the undertaking's total global turnover of the preceding fiscal year (whichever is higher).

- ***Foreign organisations may also be subject to consequences under the PIPL for violating Chinese citizens' personal information rights or harming China's national security or public interest.*** The state cybersecurity and informatization department may place offending organisations on a blacklist, resulting in restrictions on receiving personal information for blacklisted entities (*Article 42*). The PIPL does not provide clarity on what constitutes a violation of Chinese citizens' personal information rights or what qualifies as harming China's national security or public interest.

Companies operating in China should pay particular attention to the cross-border data transfer issues raised by the PIPL:

- ***Foreign organisations will need to disclose certain information when transferring personal information outside of China's borders***. Under the PIPL, PIPEs must obtain the data subject's consent prior to transfer, although the required form and method of that consent is not clear (*Article 39*). Entities seeking to transfer data must also provide the data subject with information about the foreign recipient, including its name, contact details, purpose and method of the data processing, the categories of personal information provided and a description of the data subject's rights under the PIPL (*Article 39*).

- ***Certain companies may need to undergo a government security assessment prior to cross-border data transfers.*** In addition to the consent and disclose requirements under Article 39, "critical information infrastructure operators" and PIPEs processing personal information in quantities exceeding government limits must pass a government security assessment prior to transferring data outside of China (*Article 40*). The term "critical information infrastructure operator" is not further defined within the PIPL, the term is, however, broadly defined within the newly passed Regulations on the Security and Protection of Critical Information Infrastructure (the "Regulations on Critical Information Infrastructure"), which come into effect on September 1, 2021 (the Mandarin version is available here). Under Article 2 of the Regulations on Critical Information Infrastructure, a "critical information infrastructure operator" is a company engaged in important industries or fields, including public communication and information services, energy, transport, water, finance, public services, e-government services, national defense and any other important network facilities or information systems that may seriously harm national security, the national economy and people's livelihoods, or public interest in the event of incapacitation, damage or data leaks.The PIPL also does not specify the data thresholds beyond the quantities provided by the state cybersecurity and information department or the nature of the security assessment, nor does it reference any specific legislation

issued by the state cybersecurity and informatization department for purposes of determining such data thresholds (*Article 40*).

- ***PIPEs outside China that conduct personal data processing activities for the purpose of conducting business in China or evaluating individuals' behaviour in the country must establish an entity or appoint an individual within China to be responsible for personal information issues.*** Such foreign organisations must report the name of the relevant entity or the representative's name and contact method to the departments fulfilling personal information protection duties, although the PIPL does not specify or name to which departments foreign organisations must report in such instances (*Article 53*).

- ***Companies and individuals may not provide personal information stored within China to foreign judicial or enforcement agencies, without prior approval of the Chinese government.*** As summarized in our prior client alert, the PIPL adds to a growing list of laws that restrict the provision of data to foreign judiciaries and government agencies, which could have a far-reaching impact on cross-border litigation and investigations. Chinese authorities will process requests from foreign judicial or enforcement agencies for personal information stored within China in accordance with applicable international treaties or the principle of equality and reciprocity (*Article 41*). The PIPL does not provide any guidance on how a company should seek approval if it wishes to export personal data in response to a request from a foreign government agency or a foreign court.

**IV. Next Steps**

The passage of the PIPL comes during a time where China has increased its regulatory scrutiny on technology companies and other entities with large troves of sensitive public information, and their data usage. Given the broad scope of the PIPL and its extraterritorial reach, organisations inside and outside of China will need to review their data protection and transfer strategies to ensure they do not run afoul of this network of legislation.

Even for companies that currently have GDPR compliance programs in place, the PIPL introduces new requirements not currently required under the GDPR. Examples of such requirements unique to the PIPL include, amongst others, establishing a legal entity within China and passing a security review prior to exporting personal data that reaches a certain undisclosed threshold. How the government enforces the statute and interprets its provisions remain to be seen, and a PIPL compliance program will likely require a nuanced understanding of Chinese cultural and business practices.

Companies operating in China should pay close attention to regulations, guidance documents and enforcement actions related to the PIPL as the Chinese government continues to bolster its data protection legal infrastructure, and seek guidance from knowledgeable counsel.

---

[1] Please note that the discussion of Chinese law in this publication is advisory only.

*This alert was prepared by Connell O'Neill, Kelly Austin, Oliver Welch, Ning Ning, Felicia Chen, and Jocelyn Shih.*

*Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work in the firm's Privacy, Cybersecurity and Data Innovation practice group, or the following authors:*

*Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)*
*Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)*
*Oliver D. Welch – Hong Kong (+852 2214 3716, owelch@gibsondunn.com)*

***Privacy, Cybersecurity and Data Innovation Group:***

***Asia***

*Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)*
*Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)*
*Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)*

***Europe***

*Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)*
*James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)*
*Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)*
*Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)*
*Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)*
*Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)*
*Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)*
*Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)*
*Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)*
*Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)*

***United States***

*Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)*
*S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)*
*Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)*
*Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)*
*Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)*
*David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)*
*Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)*
*Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)*
*Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)*
*Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-*

*5375, jjessen@gibsondunn.com)*
*Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)*
*H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)*
*Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)*
*Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)*
*Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)*
*Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)*
*Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)*
*Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)*
*Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)*