Davis Polk

China's personal data law comes into force accompanied by draft rules on cross-border data transfers

November 1, 2021 | Client Update | 13-minute read

Personal Information Protection Law of China (PIPL) came into effect today, containing rules comprehensively regulating personal data processing activities across all industries in and out of China. On October 29, 2021, the Cyberspace Administration of China announced for public consultation draft Measures regarding Security Assessment for Cross-border Export of Data: once promulgated, these will give effect to key requirements in the PIPL concerning transmission of personal data out of China.

Introduction

The Personal Information Protection Law of China (PIPL) came into effect on November 1, 2021. Widely viewed as the Chinese counterpart to the EU General Data Protection Regulation (GDPR), the PIPL provides for a set of rules comprehensively regulating personal data processing activities across all industries and operations such as collecting, utilizing, processing, sharing and transferring personal information (PI)[1] in and out of the People's Republic of China (PRC). On October 29, 2021, the Cyberspace Administration of China (CAC), the principal cybersecurity enforcement agency, announced for public consultation draft Measures regarding Security Assessment for Cross-border Export of Data (Draft Measures on Data Export Assessment): once promulgated, these will give effect to key requirements in the PIPL concerning transmission of PI out of the PRC.

The PIPL, among other things:

- sets out "notification and consent" as the guiding principle for processing PI;
- affords a higher degree of protection to "sensitive PI"[2];
- provides a wide range of rights for data subjects, and corresponding obligations for PI processors;
- prohibits PI processors from providing PI stored in the PRC to foreign judicial or enforcement authorities absent approval of the PRC government; and
- creates rules concerning the cross-border transfer of PI stored in the PRC.

The PIPL is the first substantive PRC national legislation dedicated to PI protection. As shown in the illustration below, prior to the enactment of the PIPL, the PRC had promulgated a series of procedural and substantive laws and regulations, including the 2017 Cybersecurity Law of the PRC (CSL) and 2021 Data Security Law of the PRC (DSL), aiming to establish a comprehensive regulatory architecture governing its cyberspace and data flow out of the PRC.

Copyright 2021 Davis Polk & Wardwell LLP

Latest key developments

Procedural and substantive PRC data laws

This client update highlights several key features of the PIPL that are worthy of immediate attention for companies possessing, processing and handling data in the PRC, including the PIPL's 1) extraterritorial application binding foreign companies (even those with no presence in the PRC) handling PI of individuals located in the PRC, 2) stringent data localization requirements, 3) imposition of detailed data compliance obligations on PI processors[3], and notably, 4) penalties for violations of the PIPL.

Highlights of the PIPL

Highlights of the PIPL are summarized below.

Extraterritorial application

Like the GDPR's reach outside of Europe, the PIPL applies not only to any processing of PI carried out in the PRC, but also the processing of PRC-based individuals' PI undertaken *outside* the PRC, where:

1. the purpose of such processing is to provide products or services to individuals within the PRC;
2. the activities of individuals within the PRC are being analyzed and evaluated; or
3. it is otherwise prescribed by law and administrative regulations. (Article 3, the PIPL).

The PIPL requires such foreign companies handling PRC-based individual's PI to set up a dedicated entity or designate a representative in the PRC to deal with PI protection matters. The names and contact details of local agents or representatives must be provided to the relevant PRC authorities. (Article 53, the PIPL).

Cross-border data transfer

The PIPL regulates cross-border transfer of PI. Mainly driven by concerns about cybersecurity and data sovereignty, the PIPL stipulates stringent requirements for the transmission of PI collected or generated domestically out of the PRC.

– **Data localization:** Critical information infrastructure operators (CIIOs) [4] and organizations processing PI that have reached threshold(s) to be prescribed by the CAC are required to store in the PRC PI that is domestically collected and generated. (Article 40, the PIPL).

Copyright 2021 Davis Polk & Wardwell LLP

- **Data Export Assessment:** where a PI processor wants to export certain PI overseas, at least one of the following criteria must be met:
- 1. the PI processor has passed the security assessment administered by the CAC (see below for details);
- 2. the PI processor has been certified by a specialized agency for PI protection pursuant to CAC's regulations;
- 3. the PI processor has entered into a standard contract (to be formulated by the CAC) with the recipient of PI; or
- 4. other circumstances provided in laws, regulations or prescribed by PRC government. (Article 38, the PIPL).

The Draft Measures on Data Export Assessment, prepared with stated objectives of standardizing data export, protecting PI, safeguarding public interest and national security, and promoting the safe and free cross border transmission of data (Articles 1), sets out the scenarios under which an application to the provincial level CAC agency is required:

1. export of personal information and critical data collected or generated by CIIOs;
2. export of any critical data[5];
3. export of PI by a PI processor who handles PI of over one million individuals;
4. export of PI belonging to over 100,000 individuals or export of sensitive PI belonging to over 10,000 individuals; and
5. other situations as determined by the CAC. (Article 4, Draft Measures on Data Export Assessment).

Under the Draft Measures, data processors are required to conduct a self-assessment of data export risk before cross-border transmission, including the necessity, and legality of the purpose, scope and method of data export and the handling of data by the overseas recipient, the potential damage to national security, public interest and legal interest of individuals and entities, the ability of the overseas recipients to safeguard the transmitted data from damage and leakage, the undertaking made by the overseas data recipients, the availability of remedy for data subjects, and the sufficiency of the data protection contract terms signed by the overseas recipient. These factors reflect the key considerations by the CAC in its data export review. (Articles 5 and 8, Draft Measures on Data Export Assessment). While it remains to be seen how this Article will be interpreted, it would seem that for one-off cross-border transmissions, the assessment needs to be conducted before the export of PI. For business operations that require continuous outbound flow of PI, it would seem that the relationship with an overseas PI recipient and the safeguards to protect the PI during and after the transmission on an ongoing basis should be scrutinized and properly documented in the export risk self-assessment.

Draft Measures provide that within 7 days of receipt of an application for data export approval, CAC will inform the applicant whether its case has been accepted for further review, with the further review to be completed in principle within 2 months. CAC's approval is valid for two years subject to its right to revoke the approval if warranted by a change of circumstances. (Articles 7, 11 and 12, Draft Measures on Data Export Assessment).

Further, the PIPL requires PI processors to adopt necessary measures to ensure that the handling of the PI by the overseas recipient reaches the standard of PI protection as set out by the PIPL. (Article 38, the PIPL).

- **Requests from foreign judiciary and law enforcement:** The PIPL is aligned with the recently adopted DSL on how to handle PI requests from foreign judicial and law enforcement (e.g., subpoenas in criminal, regulatory and civil litigation contexts outside of the PRC). The PIPL prohibits provision of PI stored in the PRC to foreign judicial or law enforcement agencies without the permission from the relevant PRC authorities. Relevant PRC authorities will act in accordance with international treaties or the principles of reciprocity. (Article 41, the PIPL).
- **Notification and consent requirement:** Specific consent must be obtained from data subjects where the PI is transferred outside the PRC. (Article 39, the PIPL). The PIPL does not provide exceptions to this requirement, and it is not clear whether specific consent from the individual would still be required if the export of such data has independently been approved by the CAC.

Data governance

A separate chapter (Chapter 5) of the PIPL sets forth details about PI processors' obligations, which include:

- **Obligations to take security measures:** the PIPL creates obligations for PI processors to adopt security measures such as establishing internal PI management policies and procedures, applying appropriate technical security measures such as cryptography and anonymization, conducting training, and creating contingency plans, to ensure PI processing is in compliance with relevant laws, and to prevent the PI from being divulged, tampered with or lost. (Article 51, the PIPL).
- **Audits:** PI processors shall regularly undertake data auditing. (Article 54, the PIPL).

Copyright 2021 Davis Polk & Wardwell LLP

- **Data breach notification:** PI processors must inform the government authorities in charge of PI protection (including, but not limited to, the CAC) when PI has been or may have been unintentionally divulged, tampered with or lost. In such cases, PI processors are obliged to take remedial measures and may be required to inform the PI subjects if the damage cannot be remediated. (Article 57, the PIPL).
- **Impact assessment:** where a PI processor is dealing with sensitive PI, utilizing PI for automatic decision making, providing PI to other PI processors, processing cross-border transfer of PI or undertaking other PI handling that may have significant impact on personal interests, the PI processor is required to assess the impact of its activity on PI protection and make a record of how such matters are decided and handled. (Articles 55 and 56, the PIPL).
- **Data protection officer**: PI processors that have processed PI in the PRC reaching threshold(s) to be prescribed by CAC shall designate a person in charge of PI protection. (Article 52, the PIPL).
- **Gatekeeper obligation:** For PI processors that provide important internet platform services, have a significant number of users and have complicated business models, the PIPL imposes special obligations on them to establish a comprehensive PI protection system and rules to ensure compliance with PI protection requirements within the platform. (Article 58, the PIPL).

Supervision and penalties

The PIPL empowers the CAC to coordinate the protection of PI and relevant supervision and administration work. (Article 60, the PIPL). Regulators overseeing sectors such as information technology, public security, finance and market order are also expected to play a supervisory role with respect to PI protection within the scope of their respective duties. Local government authorities are also given a supervisory role. The government may make inquiries of individuals, collect documents such as contracts and business records, conduct onsite inspections, and examine equipment in connection with the handing of PI. (Article 63, the PIPL).

Penalties for any violation of the PIPL by a company include a fine up to RMB 50 million (approx. US$ 7.8 million) or 5% of its turnover in the preceding year, cessation of operation and revocation of business license. Penalties against individuals include a fine up to RMB 1 million and a ban from serving in a managerial role in the organization.

The PI processor shall be liable in tort for damage suffered by a data subject unless the processor can prove absence of fault.

Our observations

- **Examination of compliance with PI protection framework**: Companies with operations or customer bases in the PRC should evaluate the extent to which the PIPL applies to both their Chinese and non-Chinese entities/operations. Further, a survey of relationships with Chinese counterparties will be helpful in managing risks as a result of potential restrictions on transmission of data from the PRC by the counterparties.
- **Consent and opt-out**: the PIPL provides very broad language in favor of data subjects' right to be sufficiently informed of the collection, processing, use and transfer of their PI. PI processors are obligated to enable opt-outs by data subjects at any stage. PI processors cannot decline to provide services to the data subjects on the grounds of their rejection of PI processors' requests for consent, unless such PI is necessary for the provision of products or services. (Article 16, the PIPL). Companies are advised to carefully review their contract terms and conditions with individuals in the PRC (including employees and customers in particular) to strike the right balance between adequate notification pursuant to the laws, on the one hand, and, on the other, flexibility in carrying out PI processing in daily business.
- **Inclusion of Chinese standard contractual clauses:** For companies that are not CIIOs and are not handling PI reaching the threshold(s) that will be designated by CAC, they may transfer PI overseas by entering into a standard contract with foreign recipients to be formulated by CAC. (Article 38, the PIPL). This approach is similar to the "Standard Contractual Clauses" approach under the GDPR. The CAC has not yet released any text of sample terms. Companies should look for the publication of service contract templates and then aim to amend their service terms if required.
- **Enhance data compliance due diligence in investments:** The PIPL's extraterritorial application and the potential for substantial fines (including up to 5% of turnover in the preceding year) necessitates thorough due diligence on a Chinese target's compliance with data protection law. Appropriate consideration must also be given to whether and how personal data can be transferred (or made available) out of the PRC, potentially complicating business consolidation goals.

Copyright 2021 Davis Polk & Wardwell LLP

– **Additional data rules to come:** The Draft Measures concerning Data Export Assessment, announced just days before the entry into force of the PIPL, provide some highly anticipated clarity on some of the most critical provisions of the PIPL. The public consultation phase will end on November 28, 2021. The above mentioned sample service contract terms are absent from the current draft. The regime for a data export certification by a specialized agency for PI protection in lieu of a CAC review is also not addressed in the draft. Further, as indicated in Article 62 of the PIPL, the CAC will coordinate with other authorities to promulgate detailed implementation rules and standards regulating small-scale PI processors, handling of sensitive PI, and technologies such as facial recognition and artificial intelligence. Future regulatory guidance is also expected regarding the threshold(s) for a PI processor's duty to appoint a data protection officer under Article 52 of the PIPL. Another draft implementation rule regarding Cybersecurity Review announced for public consultation in July 2021 is also yet to become effective. Concrete rules regarding identification of critical data are also expected, which should give further clarity and prescribe more specific obligations on the implementation of the PIPL as well as other data laws such as the DSL and CSL.[6]

Davis Polk & Wardwell LLP is not authorized to practice PRC law and the discussion in this update of PRC law and regulation are for general information only. This update is not a full analysis of the matters presented and should not be relied upon as legal advice.

Copyright 2021 Davis Polk & Wardwell LLP

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Martin Rogers
+852 2533 3307
martin.rogers@davispolk.com

Li He
+852 2533 3306
li.he@davispolk.com

James C. Lin
+852 2533 3368
james.lin@davispolk.com

Jonathan K. Chang
+1 650 752 2043
jonathan.chang@davispolk.com

Kevin Zhang
+852 2533 3384
kevin.zhang@davispolk.com

Yuan Zheng
+852 2533 1007
yuan.zheng@davispolk.com

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

1 PI is defined as information related to an identified or identifiable natural person recorded electronically or by other means, excluding anonymized information. (Article 4, the PIPL).

2 Sensitive PI is broadly defined as any information that, once leaked or used illegally, could seriously undermine personal dignity or endanger personal and property safety. Non-exhaustive examples provided in the PIPL include biometrics, religious beliefs, medical health, financial records, individual whereabouts, and information of minors under the age of 14. (Article 28, the PIPL).

3 PI processor is defined as the organization or individual that independently decides the purpose and methods when processing PI. (Article 73, the PIPL). PI processing is defined as the collection, storage, utilization, modification, transfer, provision, disclosure, deletion, etc., of PI. (Article 4, the PIPL).

4 CIIOs is a concept first unveiled in the 2017 CSL. Under article 2 of the Regulations for Safe Protection of Critical Information Infrastructure, effective from September 1, 2021, CIIOs refer to important network facilities and information systems in industries such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defense, any damage, dysfunctionality or data leak with respect to which would seriously endanger national security, the economy, and people's livelihood. Companies designated as CIIOs are subject to more stringent data security requirements and a higher level of government oversight.

Copyright 2021 Davis Polk & Wardwell LLP

[5] Critical Data is a concept first introduced in the CSL. It is not defined in any of legislation currently in force. Based on several draft implementing rules not yet in force, critical data is generally understood to be data distinguished from PI or state secrets yet pertaining to national security, economic development, social stability or public interests, the alteration, destruction, leakage or divulgence of which data may undermine national interests.

[6] Specific industry rules regulating data security have already been promulgated. See, for instance, Provisions on Management of Automotive Data Security (Trial), effective Oct 1, 2021; and Information Security Technology - Guide for Healthcare Data Security, effective July 1, 2021.

Copyright 2021 Davis Polk & Wardwell LLP