DATA PROTECTION LAWS OF THE WORLD

China

Downloaded: 25 February 2022
CHINA

LAW

There is not a single comprehensive data protection law in the People’s Republic of China (PRC). Instead, rules relating to personal information protection and data security are part of a complex framework and are found across various laws and regulations. That said, the three main pillars of the personal information protection framework in the PRC are the Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL).

On June 1, 2017, the CSL came into effect and became the first national-level law to address cybersecurity and data privacy protection. The DSL came into force on September 1, 2021, and focuses on data security across a broad category of data (not just personal information). Most significantly, the PIPL came into effect on November 1, 2021. The PIPL is the first comprehensive, national-level personal information protection law in the PRC. The PIPL does not replace – but instead enhances and clarifies - earlier personal information laws and regulations.

In addition to the PIPL, CSL and DSL, the following form the backbone of general personal information protection framework currently in the PRC:

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision);
- National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services, effective from February 1, 2013;
- The Draft Regulation of Network Data Security Management, published for consultation in November, 2021; and

In the past five years, there has also been an abundance of implementing regulations and guidelines (herein referred to as Guidelines) proposed, issued or revised to flesh out the essentials and concepts introduced under the personal information protection framework. These include, non-exhaustively:

- Guidelines on Internet Personal Information Security Protection, effective from April 19, 2019; and

The Decision has the same legal effect as law, and its purpose is to protect online information security, safeguard the lawful rights and interests of citizens, legal entities or other organizations, and ensure national security and public interests. While the PIS Specification and other Guidelines are only technical guides (covering in detail key issues such as data transfers, sensitive personal information and data subject rights), and thus not legally binding, they have historically been highly persuasive. Given the recent promulgation of the PIPL, the PIPL will now take precedence over the PIS Specification and other Guidelines. Nonetheless, the PIS
Specification and the Guidelines are still useful for the purposes of supplementing legislation, especially on any part that has not been addressed by the PIPL, CSL or DSL. In addition to all of the above:

- provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law have generally been used to interpret data protection rights as a right of reputation or right of privacy. However, such interpretation is not explicit. Further, the PRC Civil Code, effective on January 1, 2021 also further reinforces the statutory right of privacy for individuals and establishes data protection principles; and
- provisions contained in other laws and regulations may also apply depending on the industry or type of information involved (for example, personal information obtained by financial institutions and e-commerce businesses, personal information collected by telecom or Internet service / content providers, healthcare and genetic information, etc.). Applicability of other laws or regulations (including provincial level laws), such as the PRC Criminal Law, PRC E-Commerce Law, PRC Consumer Rights Protection Law and the new data law in Shenzhen, will invariably depend on the factual context of each case and further independent analysis is recommended.

Given the personal information protection framework is still evolving, and further regulations accompanying the new PIPL and DSL are anticipated to be published in the coming months, it is recommended that organizations continue to monitor the developments of the PRC data protection regulatory framework.

**Extra-territorial scope**

The PIPL has extra-territorial effect, and applies both to:

- data processing activities within the PRC; and
- processing of PRC residents’ data outside of PRC where:
  - for the purposes of providing products or services to PRC residents;
  - for analytics or evaluation of behavior of PRC residents; or
  - for any other reasons as required by law or regulations.

The PIPL applies to both the public and private sectors.

**DEFINITIONS**

**Definition of personal data**

The PIPL defines personal data as any kind of information relating to an identified or identifiable natural person, either electronically or otherwise recorded, but excluding information that has been anonymized.

**Definition of sensitive personal data**

The PIPL defines sensitive personal data as information that, once leaked or illegally used, will easily lead to infringement of human dignity or harm to the personal or property safety of a natural person, including (but not limited to): (i) biometric data; (ii) religion; (iii) specific social status; (iv) medical health information; (v) financial accounts; (vi) tracking/location information; and (vii) minors data.

**NATIONAL DATA PROTECTION AUTHORITY**

The PIPL has now clarified that the Cyberspace Administration of China (CAC) is primarily responsible for the overall planning and coordination of personal information protection and related supervision. Prior to the PIPL coming into force, various other legislative and administrative authorities have also claimed jurisdiction over data protection matters, and may continue to play some form of role in the context of personal information protection, such as:

- National People's Congress Standing Committee
- Ministry of Public Security
- Ministry of Industry and Information Technology
- State Administration for Market Regulation
Data Protection Laws of the World

China

Notwithstanding the CAC’s newly-clarified role, sector-specific regulators, such as the People’s Bank of China or the China Banking and Insurance Regulatory Commission, may also monitor and enforce data protection issues of regulated institutions within their sector.

REGISTRATION

Generally, there is no legal requirement in the PRC for data users to register with the data protection authority. That said, there are specific registration requirements imposed on the sharing and transferring of specific categories of data (e.g. human genetic resources), and proposed filing requirements for security impact assessments (see Cross Border Transfers).

DATA PROTECTION OFFICERS

Under the PIPL, organisations which meet certain data processing volume thresholds (as yet unspecified by the CAC) are required to appoint a Data Protection Officer (DPO), and to register the name(s) and contact details of the responsible person with the relevant data protection authority.

For organisations based outside of the PRC, but processing PRC personal information, a specific representative or organisation within the PRC should be appointed, and details reported to the data protection authority.

Details of how and when the DPO or representative (as the case may be) should be registered is awaited.

Whilst the authorities have yet to announce the volume threshold for DPO requirements applicable under the PIPL, the PIS Specification requires an organization to appoint a data protection officer and a data protection department if the organization:

- has more than 200 employees and its main business line involves data processing;
- processes personal information of more than 1,000,000 individuals, or is estimated to process personal information of more than 1,000,000 individuals; or
- processes sensitive personal information of more than 100,000 individuals.

COLLECTION & PROCESSING

Consent

In general, express, informed consent is required from the data subject before personal information can be collected, used, transferred or otherwise processed. In certain circumstances, such as collecting or processing sensitive personal information, overseas data transfers and direct marketing, explicit consent (i.e. consent specific to the processing activity / transfer (rather than just general consent to the privacy notice, expressed through an affirmative action) is required from the data subject. Collection from individuals under 14 years old is prohibited unless explicit consent is obtained from their legal guardians. As a matter of best practice, explicit consent is recommended.

In addition, the PIPL has introduced a new requirement for separate consent to be obtained for:

- processing sensitive personal information;
- overseas transfers;
- public disclosure of personal information;
- to provide data to another data controller for processing; and
- use of image or identification data collected in public through image or identification device for purposes other than maintaining public security.
Whilst there is no clear definition of what “separate consent” constitutes in practice, it appears to suggest that organisations should avoid bundled or forced consent.

The PIPL also introduced limited circumstances (i.e. lawful bases) in which personal information can be processed without consent, including:

- entering into or fulfilling a contract where the data subject is a named party;
- carrying out human resources management under an employment policy legally established or a collective contract legally concluded;
- fulfilling legal obligations (which may be helpful in the context of regulatory investigations);
- in response to public health incidents;
- for public security and public interest reasons; and
- as required by law (e.g. where required to disclose information under another PRC law).

However, in practice, it is unclear how these lawful bases could be relied upon. Consent remains the primary basis for lawful data processing, and it is anticipated this will continue in practice.

**Notice**

In addition to obtaining consent, a data controller (i.e. the organization who has the authority to determine the purposes, means or method of processing) should provide data subjects with a privacy policy or other form of notice, informing them of the scope and ways in which their personal information is collected, processed and disclosed, including the following information:

- the identity of the data controller, including its registered name, registered address, principal office, a telephone number and / or an e-mail address;
- a list of personal information collected for each business purpose. Where sensitive personal information is involved, relevant consent shall be explicitly marked or highlighted;
- the location of storage, retention period, means of use / processing and scope of the personal information collected;
- the purposes sought by the data controller, i.e. what the data controller uses the data for (for instance, supplying goods and services, creating a user account, processing payments, managing subscriptions to the newsletters, etc.). These should be as comprehensive as possible, as additional purposes will require new consent;
- circumstances under which the data controller will transfer, share, assign personal information to third parties (including intra-group entities) or publicly disclose personal information, the types of personal information involved in these circumstances, the types of third party data recipients, and the respective security and legal responsibilities of the entities;
- the rights of data subjects and mechanisms for them to exercise such rights, e.g. methods to access, rectify or delete their personal information, to de-register their accounts, withdraw their consent, obtain copies of their personal information and restrict automated decision by the data system etc.;
- potential risks for providing personal information, as well as possible consequences for not providing the data;
- data security capabilities of, and data security protection measures to be adopted by, the data controller and, when necessary, the compliance certificates related to data security and personal information protection; and
- channels and procedures for making inquiries and lodging complaints by data subjects, as well as external dispute settlement body and contact information.

The information in the privacy policy must be true, accurate and complete. The contents of the privacy policy must be clear and easy to understand, and ambiguous language should be avoided. The privacy policy should be made available to the data subject when collecting consent, and published publicly and easily accessible, for example, through a link placed prominently on a webpage or an installation page of a mobile application. When changes occur to the information provided in the privacy policy, the data subjects should be notified of such changes and (depending on the extent of changes made) further consent may need to be obtained.
Processing

Collection and processing of personal information must be directly related to the purpose of processing specified in the privacy notice.

Excessive data collection must be avoided. Interestingly, the provisions of the PIPL around data minimization appear to be targeted at apps and big data analytics. Additional restrictions are placed on use of biometric data collected in public places.

There are prohibitions on illegal collection, use, processing, sale, disclosure and transfer of personal information.

Impact assessment and record-keeping

The PIPL requires data controllers to undertake personal information impact assessments (PIIA) and to retain the results and processing records (for three years) in the following circumstances:

- processing of sensitive personal information;
- using personal information to conduct automated decision-making;
- appointing a data processor;
- providing personal information to any third party (likely to include sharing with group companies);
- public disclosure of personal information;
- overseas data transfer of personal information; and
- any other processing activities that may have "significant impact to an individual".

A PIIA should include an assessment on:

- whether the purpose of use and means of processing is legitimate, proper and necessary;
- impacts and risks to individual's interests; and
- applicability of protection measures and risk appetite.


TRANSFER

If a data controller wishes to share, disclose or otherwise transfer an individual's personal information to a third party (including group companies), the data controller must:

- inform the data subject of the purposes of the sharing, disclosure or transfer of the personal information and the types of data recipient, and obtain prior express consent from the data subject;
- perform a personal information impact assessment (PIIA), and take effective measures to protect the data subjects according to the assessment results (e.g. putting in place a data transfer agreement or similar contractual protections) (see Collection & Processing);
- record accurately and keep the information in relation to the sharing, disclosure or transfer of the personal information, including the date, scale, purpose and basic information of the data recipient of the sharing or assigning;
- ensure personal information is only transferred where required for processing purposes;
- not share or transfer any personal biometric information or other types of particularly sensitive personal information where prohibited under relevant laws or regulations; and
- ensure contractual measures are entered into to require the data processor to comply or assist the data controller in complying with obligations under data protection laws.

Cross-border transfers

The PIPL provided helpful clarification (after years of uncertainty) on the issue of cross-border data transfers and data localization in the PRC. In short, most personal information can be transferred or accessed outside of the PRC providing the following compliance steps are taken:
one of the following criteria is fulfilled:
- the organisation has passed a CAC security evaluation;
- the organisation has obtained certification from a CAC-accredited agency;
- the organisation has put in place CAC standard contractual clauses (not yet published) with the data recipient – likely to be most relied upon in practice; or
- for compliance with laws and regulations or other requirements imposed by the CAC;
- the data controller has adopted necessary measures to ensure the data recipient’s data processing activities comply with standards comparable to those set out in the PIPL. In practice this means initial due diligence, sufficient contractual protections and ongoing monitoring etc.;
- notice and separate, explicit consent has been given/obtained (see above) from the data subject (see Collection & Processing); and
- a PIIA has been conducted (see Collection & Processing).

The PIPL does not include a specific requirement to keep copies of personal information in the PRC, but the regulators’ expectations in this regard may remain.

However, certain personal information (and non-personal data) must still remain in (and cannot be accessed outside of) the PRC. This includes (this is not an exhaustive list):

- personal information processed by critical information infrastructure operators (CIIOs), unless a CAC-conducted security assessment has been completed;
- personal information processed by data controllers above a threshold/volume to be identified by the CAC (not yet finalised), unless a CAC-conducted security assessment has been completed;
- certain data under industry-specific regulations (such as in the financial services sector and genetic health data); and
- certain restricted data categories (such as “state secrets”, some “important data”, geolocation and online mapping data etc.).

Lingering uncertainty remains about the need for a CAC-conducted security assessment in certain situations. The Draft Guidelines on Overseas Transfer (published in November 2021) proposes a host of scenarios where this may be the case, including: personal information processed in the context of certain listing/corporate/restructuring activities; and processing of large volumes of personal information and/or sensitive personal information. The Draft Network Data Security Management Regulation also proposes introducing annual data overseas transfer security report to the CAC as well as other record keeping requirements. As such, organizations should keep developments under review.

Finally, according to the PIPL:

- a new publicly-available entity list may be published, listings foreign organisations to whom local PRC organisations may not transfer personal information, where such transfer may harm national security or public interest;
- data controllers must not provide personal information stored within China to overseas legal or enforcement authorities unless approval is obtained from a designated Chinese authority. It remains unclear whether this extends to, say, requests from overseas industry regulators; and
- the PIPL clarifies that Chinese authorities may provide personal information stored within China to overseas legal or enforcement authorities upon request, if and to the extent that there are international treaties or regulations in place to maintain fairness and for mutual benefit.

**SECURITY**

According to the CSL, DSL and PIPL, organizations must keep personal information confidential and establish a data security management system. This includes taking appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal information. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data. Security measures must be deployed, as prescribed by the CSL and DSL and
their underlying measures, guidelines and technical standards (including the TC260 guidelines). The PIPL includes a specific obligation on data controllers to adopt corresponding encryption or deidentification technologies, and to adopt access controls and training.

Systems should also be established to handle complaints or reports about personal information security, publish the means for individuals to make such complaints or reports, and promptly handle any such complaints or reports received. Organizations must conduct mandatory data/cyber security training.

Additional security safeguards must be applied to processing of sensitive personal information and organizations deemed CIIOs (see above).

The CSL implemented a multi-level protection scheme for cybersecurity protection of information systems by network operators. Information systems are classified into 5 tiers and the security standard goes higher from tier 1 to tier 5. Organizations should conduct a self-evaluation and determine the tier(s) to which its information systems belong, based on relevant laws, regulations and guidelines. Filing to the Public Security Bureau is required and, in certain circumstances, assessment by accredited third party may also be required, depending on the determined tier level of a respective information system. Further national standards and guidelines have been published to provide further details and requirements on the process and technical aspect of the tiered system. The DSL proposes introducing a similar tiered-security scheme for classification of data in due course (details have not yet been published).

If a data controller appoints a data processor to process personal information on its behalf, the data controller should ensure sufficient measures are adopted by the data processor to protect the personal information: for example, to conduct due diligence and regular audits on data processor to ensure the data processor adopts sufficient and adequate security measures; and put in place an appropriate data processing agreement with the data processor.

**Breach Notification**

Breach notification requirements are contained in the CSL, DSL and PIPL, and should be read together. “Network security incidents” that are notifiable are defined by reference to seven categories of different incident types. Guidelines set out other factors that should be considered whether a network security incident is potentially reportable. The China National Internet Emergency Center may be contacted in case of doubt as to whether an incident is potentially reportable.

An incident must be immediately notified: (i) internally, to the DPO; and (ii) externally, to the regulator (the PIPL refers to the CAC establishing (local) “personal information protection departments” (PIPD) for such purposes, but this is yet to be confirmed), and should include:

- affected data categories;
- reasons for the incident, and potential consequences;
- remedial measures, and mechanisms required by data controller to minimize impact; and
- contact information for data controller.

If the data controller can effectively avoid the disclosure, loss or tampering of data, the PIPL suggests that there is no need to notify data subjects. Otherwise (and as per the CSL and DSL) data subjects must be notified immediately if the actual or suspected network security incident may result in harm to the rights and interest of the affected data subjects. Further, if the PIPD believes it may cause impact to individuals, they may request that the data controller notifies individuals. Similar information must be given to the data subjects alongside advice on how to protect against risks arising from the incident.

Further changes are also expected in this regard. Notably, the Draft Network Data Security Management Regulation (intended to supplement the PIPL) clarifies that incidents involving any of the following must be notified to the CAC and other relevant regulators within eight hours of the data incident:

- personal data of more than 100,000 individuals; or
- any important data.

A second report to the CAC is then required within five working days of the incident being resolved.
In any case, immediate remedial action must be taken in the event of any suspected or actual data disclosure, loss or tampering.

Organizations should also adopt proactive measures to minimize the risk of personal information breaches or security incidents, including but not limited to, implementing and testing a data incident contingency plan and organizing training.

We understand the regulators are working on a project to publish further guidelines as to how network security incidents should be managed.

**ENFORCEMENT**

Possible enforcement of, and sanctions for, a data protection breach in the PRC will depend on the specific data protection laws and regulations breached. Sanctions in relation to data protection breaches are scattered across various different laws and regulations, and the measures described below may not be comprehensive in all situations, as additional laws or regulations may be applicable depending on the industry or type of information at hand.

Taking the PIPL by way of example, it provides a range of sanctions, including (inter alia):

- enforcement notices and warnings;
- administrative fines of up to (for the most serious offences) 5% of the previous year’s annual revenue (unclear if local or global revenue) or up to RMB million, and confiscation of unlawful income. Note the PIPL imposes much higher fines than under other existing data privacy regulations);
- cessation of processing;
- suspension of apps and/or services;
- suspension of business;
- suspension of management/officials role;
- criminal sanctions (for certain offences, and under relevant criminal laws);
- civil claims;
- social credit score or equivalent business credit files may be affected.

While the PIPL has now introduced higher fines, we anticipate that in practice the operational and contractual risks faced by organisations not complying with China’s data privacy framework – alongside increasing reputational risks – remain very significant and should be managed very carefully.

**ELECTRONIC MARKETING**

Direct marketing by electronic means is only possible if the targeted consumers have explicitly consented to receiving such messages either at the time their electronic address / mobile phone number was collected or at a later time.

Specific information must be stated in each electronic message: for example, the identity of the entity sending the message, and a mark identifying “Guang ago” (which means advertisement in Chinese) or “AD” on a direct marketing message.

There are also specific rules applicable to direct marketing by text messages (SMS), and certain specific prescribed information must be provided to data subjects at the time their mobile phone number was collected or prior to sending direct marketing text messages.

**ONLINE PRIVACY**

The general compliance obligations applicable to processing of personal information under the PIPL apply to the online (and offline) environments. In addition, the PIPL imposes additional compliance obligations on organisations that fall into one of the following categories:

- “important internet platform providers”;  
- data controllers processing data of a “large volume of users”; or  
- “complex businesses”.

It is still unclear which organisations would fall within these categories, but these organisations must comply with additional
measures when processing personal information, namely:

a. set up personal information protection compliance mechanisms;
b. set up external independent data protection organisations to supervise data protection mechanisms;
c. establish platform regulations;
d. establish and publish processing obligations and processing rules that regulate products and service providers in an open and fair manner;
e. stop the provision of products or service providers if they violate the law or regulations as regards processing of personal information; and
f. publish from time to time social responsibility reports as regards processing of personal information.

In terms of automated-decision making and profiling:

- analytics or evaluation based on computer programme around behavior, interests, hobbies, credit information, health or decision making activities, must be transparent, open and fair, and should not apply any differential treatment between individuals; and
- any push information or business marketing should not be directed to an individual’s character and should provide individuals with a convenient way to opt out.

As well as the PIPL, the CSL, Consumer Protection Law and E-Commerce Law offer protection to consumer / user personal information. As well as personal information protection, under these rules data controllers should strengthen management of information provided by users, prohibit the transmission of unlawful information and take necessary measures to remove any infringing content, then report to supervisory authorities. Sufficient notice and adequate consent should be obtained from data subjects prior to the collection and use of personal information. Further obligations are imposed on mobile apps providers including but not limited to conducting real-name identification, undertaking information content review.

In recent years, the regulators have also issued a range of guidelines targeting mobile app providers. These guidelines introduce specific data protection and privacy obligations aiming to regulate the data collection practices and processing activities of mobile app providers. There has also been a crackdown against (suspected) non-compliant mobile apps. Organisations are advised to review their app compliance as a matter of priority.

Data subject rights (under the PIPL and other laws within the personal information framework), include rights to access and obtain information about their data held and processed, to correct their data, to request deletion of data in the event of a data breach, to object to automated decision-making and to de-register their account etc. Most importantly is the right to withdraw consent to personal information processing.

There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC. However, the use of cookies and / or similar tracking technologies, to the extent they constitute processing of personal information, should be notified to data subjects as part of a privacy policy and adequate consent should be obtained from data subjects for such use.

Further information

See our Navigating China series for more information on China’s evolving cybersecurity and data protection landscape.
KEY CONTACTS

Carolyn Bigg  
Partner, Global Co-Chair of Data Protection, Privacy and Security Group  
T +852 2103 0576  
carolyn.bigg@dlapiper.com

Venus Cheung  
Registered Foreign Lawyer  
T +852 2103 0572  
venus.cheung@dlapiper.com

Fangfang Song  
Consultant  
T +86 1085200673  
fangfang.song@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.