DATA PROTECTION LAWS OF THE WORLD

China

DLA PIPER

Downloaded: 17 January 2022

CHINA

Last modified 25 January 2021

LAW

There is not a single comprehensive data protection law in the People's Republic of China (PRC), although one has now been proposed (see below). Instead, rules relating to personal information protection and data security are part of a complex framework and are found across various laws and regulations. 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.

On June 1, 2017, the PRC Cybersecurity Law came into effect and became the first national-level law to address cybersecurity and data privacy protection. Following this, there has 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 PRC Cybersecurity Law. These include, non-exhaustively:

- National Standard of Information Security Technology – Personal Information Security Specification (PIS Specification), as amended and effective from October 1, 2020;
- Guidelines on Internet Personal Information Security Protection, effective from April 19, 2019; and
- National Standard of Information Security Technology – Guidelines on Personal Information Security Impact Assessment, effective from June 1, 2021.

In addition to the PRC Cybersecurity Law, the following form the backbone of general data protection rules currently in the PRC:

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision) and
- 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 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 are highly persuasive. Given the lack of binding laws and regulations which provide detailed guidance on data processing, the PIS Specification and other Guidelines are important references. Therefore, compliance with the PIS Specification and other Guidelines is recommended as best practice.

Apart from the PRC Cybersecurity Law and the Guidelines, the PRC Civil Code, effective on January 1, 2021 also further reinforces the statutory right of privacy for individuals and establishes data protection principles.

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, will invariably depend on the factual context of each case and further independent analysis is recommended. Consideration should also be given to the draft PRC Data Security Law, which was published for consultation on July 3, 2020 and, if passed, would create new data security management responsibilities for organizations.

On October 21, 2020, a draft PRC Personal Information Protection Law (Draft PIPL) was published for consultation. If passed, the Draft PIPL would be the first comprehensive national level personal information protection law in the PRC, creating binding compliance obligations previously considered recommended practice (under the Guidelines), and requiring organizations to comply with new compliance steps. It remains unclear when the Draft PIPL will be promulgated, though further draft(s) are anticipated and likely before it is finalized. It is recommended that organizations continue to monitor the developments of the PRC data protection regulatory regime.

DEFINITIONS

Definition of personal data

There is no single, pervasive definition of personal data in the PRC, but the concept of personal data in the various laws, regulations and guidance that comprise the data protection framework in the PRC are starting to become more aligned.

In summary, personal data (which is generally referred to as "personal information" in the PRC) means all kinds of information (including sensitive personal information) recorded by electronic means or otherwise that can be used to independently identify or be combined with other information to identify a natural person's information.

Definition of sensitive personal data

Similar to personal information, there is no single, pervasive definition under binding laws in the PRC for sensitive personal data (which is generally referred to as "sensitive personal information" in the PRC).

However, the PIS Specification – which as noted above is a non-binding, highly persuasive standard – provides some distinction between sensitive personal information and general personal information. Sensitive personal information is defined in the PIS Specification as personal information which, if disclosed or abused, will lead to adverse impact to the data subject. Examples of sensitive personal information as set out in the PIS Specification include personal identification number, mobile phone number, individual biometric information, bank account number, correspondence records and contents, property information, credit information, location tracking, lodging information, health and physiological information and transaction information etc. The Draft PIPL also defines sensitive personal information in a similar manner.

NATIONAL DATA PROTECTION AUTHORITY

There is no single PRC regulatory authority which deals exclusively with data protection / privacy matters. The Cyberspace Administration of China (CAC) is currently generally considered the primary data protection authority in the PRC, although various other legislative and administrative authorities have claimed jurisdiction over data protection matters, such as:

- National People's Congress Standing Committee
- Ministry of Public Security
- Ministry of Industry and Information Technology
- State Administration for Market Regulation
- Ministry of Science and Technology

Other 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.

Based on its wording as at October 21, 2020, the Draft PIPL may introduce a new data protection authority(ies) by joining the CAC with the relevant data protection departments under local people's governments at or above the county level. Organizations

should monitor developments in this regard.

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 filling requirements for security impact assessments (see section on Cross Border Transfers).

The Draft PIPL would, if implemented, introduce registration requirements for organizations which:

- meet certain data processing volume thresholds (as yet unspecified by the CAC) to designate a person in charge of personal information protection and register the name(s) and contact details of the responsible person with the relevant data protection authority; or
- are outside the PRC to establish a dedicated entity or appoint a representative within the PRC and register the name(s) and contact details of the relevant entity or representative with the relevant data protection authority.

DATA PROTECTION OFFICERS

There is no general requirement under binding PRC laws for organizations to appoint a data protection officer.

However, 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 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, specific 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. As a matter of best practice, and given the wide definition of sensitive personal information, explicit consent is recommended.

The Draft PIPL would, if passed in its current form, introduce 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;
- 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.

It is important to note that the formalities for obtaining consent would also be changed under the Draft PIPL if implemented, in that, "separate consent" (as yet unspecified) must now be obtained for sensitive personal information, disclosures to third parties, public disclosures, collection of image or identification information (i.e. biometric data) and for overseas data transfers.

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 further consent may need to be obtained.

While it is recommended best practice under the PIS Specification for data controllers to establish a personal information impact assessment system to assess security risks associated with personal information processing activities and identify effective protection measures, the Draft PIPL would, if implemented in its current form, specifically require data controllers to undertake personal information impact assessments (PIIA) and to retain the results (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".

The National Standardization Technical Committee for Information Security has published the "Guidance for Personal Information Security Impact Assessment" (PIIA Guidelines) which will be implemented on June 1, 2021.

Collection from individuals under 14 years old is prohibited unless explicit consent is obtained from their legal guardians.

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; and
- not share or transfer any personal biometric information or other types of particularly sensitive personal information where prohibited under relevant laws or regulations.

Cross-border transfers

Where the sharing, disclosure or transfer of the personal information is to a third party outside of the PRC, additional rules will apply. Data localization is an increasing trend in the PRC, with various draft measures as well as sector-specific regulations prohibiting the transfer of certain personal information outside the borders of the PRC. Although to what extent these rules apply remains unclear and further clarification from the regulators is expected, there has been more guidance published by certain regulators for example on healthcare data and the specific requirements on human genetic data. We anticipate more to come in the upcoming year.

Under the current prevailing understanding, in order to transfer or access personal information outside of the PRC, the data controller must:

- inform the data subject of the cross-border transfer, and obtain explicit consent of the data subject before the personal information is shared, disclosed, transferred or accessed overseas;
- store a copy of the data within the PRC; and
- conduct a security assessment (in addition to the personal information impact assessment (PIIA) described above), which is likely to be a self-assessment

On June 13 2019, the CAC circulated for public comment the Measures on Cross Border Transfer Security Assessment (Measures). The Measures introduced a range of activities that organizations should undertake prior to overseas transfers, including non-exclusively:

- all network operators (and not just critical information infrastructure operators (CIIO)) will now have to undertake a security assessment before transferring personal overseas, and file this with the local CAC;
- establish data transfer agreements with all offshore data recipients and ensure sufficient contractual safeguards;
- submit annual report to the CAC on the status of cross border transfers and the performance of data transfer agreements;
- maintain a log of all cross border transfers of personal information for at least give years;
- establish and maintain an effective incidental response plan and report all major data security incidents; and
- appoint a designated officer to take control and address compliance with data protection and security requirements, and to liaise with relevant authorities.

In addition to the above requirements, additional restrictions apply to transfers of certain types of information outside of the PRC, for example (this is not a comprehensive list):

- certain categories of regulated (personal and non-personal) data are not permitted to leave the PRC at all, such as state secrets;
- the People's Bank of China (PBOC) requires all onshore banks to store, handle and analyse personal financial information collected in China, and not transfer abroad such data unless otherwise permitted by law or approved by the PBOC;
- all medical, health care, and family planning service entities are required to store population and health information on onshore servers; and
- data relating to human genetic resources cannot be transferred abroad without the approval of the Ministry of Science and

Technology.

If it were to be implemented in its current draft form, the Draft PIPL reiterates the existing regulatory obligations and further introduces new obligations with respect to cross-border data transfer, as follows:

- obtain explicit data subject consent;
- undertake a PIIA (see Collection & Processing); and
- satisfy one of the below requirements:
    - put in place a contractual obligations with the data processor that meets the standards stipulated in the Draft PIPL; or
    - conducts a security impact assessment which has been approved by the CAC; or
    - obtain a personal information protection certification via a certification body accredited by the CAC (it remains unclear if this certification is available per transfer or per organization).

Under the Draft PIPL, organizations that are: (i) designated as CIIOs, (ii) national authorities, or (iii) data controllers meeting certain data processing volume thresholds (as yet unspecified) would only be able to access or transfer personal information outside of the PRC if they have conducted a security assessment which has been approved by the CAC, otherwise the personal information in question cannot be transferred or accessed overseas. It is unclear from the Draft PIPL whether retaining a local copy of the data in the PRC is also still generally required. However, industry-specific data localization rules, and prohibitions of overseas transfers of certain other restricted (personal and non-personal) data, such as state secrets and "important data", will remain. Organizations are recommended to monitor developments.

SECURITY

Organizations must take 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.

Under the PRC Cybersecurity Law, network operators (i.e. organizations that own or operate IT networks / infrastructure and, it is thought, even just websites in the PRC) must implement technical and other necessary measures to ensure the security of personal information and to prevent the data from being accidentally disclosed, tampered with or destroyed. Remedial measures must be taken immediately if personal information is being or is likely to be disclosed, tampered with or destroyed. Network operators should also establish systems 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 deemed CIIOs (see above) must apply additional security safeguards.

The PRC Cybersecurity Law 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.

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

The PRC Cybersecurity Law introduced a general requirement for the reporting and notification of actual or suspected personal information breaches. Where personal information is leaked, lost or distorted (or if there is a potential for such incidents),

organizations must promptly take relevant measures to mitigate any damage and notify the relevant data subjects and report to the relevant government agencies in a timely manner in accordance with relevant provisions.

Failure to report could result in warnings and orders of rectification being issued by the regulatory authority. In addition, administrative fines of up to RMB 100,000 against the organization and RMB 50,000 against the responsible person could apply where the offence is severe (e.g. hazardous to cyber security).

The PRC Cybersecurity Law does not provide guidance on what constitutes a data security breach, nor does it prescribe a timeline for reporting personal information breaches or security incidents. However, the PIS Specification and other guiding circulars (such as the National Network Security Incident Contingency Response Plan), and the latest draft guidelines published by the CAC on the Administrative Measures for the Release of Information on Cyber Security Threats provide some guidelines on the reporting and notification of personal information breaches or security incidents. Nevertheless, these supplementary guidelines do not go further to provide a complete set of reporting procedures.

Organizations should also adopt proactive measures to minimize the risk of personal information breaches or security incidents, including but not limited to, formulating a contingency plan, organizing trainings and conducting regular contingency drills.

The Draft PIPL would, if implemented in its current form, reinforce the mandatory data breach reporting requirement under the PRC Cybersecurity Law. However, under the Draft PIPL, notifications to affected data subjects would not be required if the data controller adopts measures that can effectively prevent any harm resulting from such data breach. Organizations are advised to monitor developments in this regard.

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.

Generally, the civil and criminal sanctions and administrative penalties for data protection breaches include warnings, orders to rectify, fines, confiscation of unlawful income, compensation to victims, cancellation of licences, prison sentences, closing down of websites and prohibition on engaging in certain types of business in the future.

Typically, it would be a graded approach – warning and requirement to comply, then possibly fines up to approximately RMB 500,000. Affected individuals may also potentially claim for indemnification under the Tort Liability Law. In severe cases, breaches may lead to higher fines being imposed or the revocation of license. Responsible personnel could be prohibited from engaging in relevant business and their conduct could be recorded in their social credit files. Depending on the severity of the illegal conduct, the responsible person could also be subject to detention or up to seven years of imprisonment, plus a concurrent fine to the organization if applicable.

The enforcement environment is evolving rapidly as individuals are increasingly aware of their data protection rights and as data protection obligations expand as laws develop and are added in the PRC. For example, the PRC Cybersecurity Law suggests the possibility of ordering corrections, issuing warnings, confiscation of illegal gains and fines of up to 10 times of illegal gains (or fines of up to RMB 1,000,000 where there is no illegal gain) upon discovery of violation in handling personal information. The responsible persons may also be fined between RMB 10,000 to 100,000.

The Draft PIPL proposes to enhance the regulators' powers of enforcement and increase the level of fines to a maximum of 5% of an organization's previous financial year's annual turnover (unclear if global or national turnover) or RMB 50,000,000. Organizations are recommended to keep monitoring developments in this aspect.

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 gao*" (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 PRC Cybersecurity Law, Consumer Protection Law and E-Commerce Law offer similar protection to consumer / user personal information. 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 the past year, the regulators have 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.

Under the PRC Cybersecurity Law, PRC Consumer Protection Law, PRC E-Commerce Law and the PIS Specification, data subject have specific rights, such as, to access their data, to correction of their data, to request deletion of data in the event of a data breach, to de-register their account etc. The same rights would be available to data subjects under the Draft PIPL (if passed), and the circumstances in which deletion of personal information can be requested would also be clarified.

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.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2021 DLA Piper. All rights reserved.