DATA PROTECTION LAWS OF THE WORLD

China

DLA PIPER

CHINA

Last modified 29 April 2024

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. Draft Amendments to the CSL were issued on September 12, 2022, proposing enhanced liabilities for violating obligations of general network operation security, security protection of critical information infrastructure, network information security and personal information protection, etc.

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);
- The Draft Regulation of Network Data Security Management, published for consultation on November 14, 2021;
- The Measures for the Security Assessment of Outbound Data Transfers, effective from September 1, 2022;
- The Measures for the Standard Contract for the Outbound Transfer of Personal Information, effective from 1 June 2023; and
- The Regulations on Facilitating and Regulating the Cross–border Data Transfers, effective from 22 March 2024.

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:

- 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;
- National Standard of Information Security Technology — Guidelines on Personal Information Security Impact Assessment, effective from June 1, 2021;

- Draft National Standard of Information Security Technology — Requirements for Classification and Grading of Network Data, published for consultation on September 14, 2022;
- Practicing Guidelines for Network Security Standards — Technical Specification for Certification of Personal Information Cross-border Processing Activities (V2.0), effective from December 16, 2022;
- Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong– Macao Greater Bay Area (Mainland, Hong Kong), effective from 10 December 2023;
- Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information (Second Edition), effective from 22 March 2024; and
- Guidelines on Application of Security Assessment of Cross-border Data Transfers (Second Edition), effective from 22 March 2024.

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. Although the PIPL takes precedence over the PIS Specification and other Guidelines, 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 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. The PRC Civil Code, effective on January 1, 2021 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 local data laws at a provincial level 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 information 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 information 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):

- biometric data;
- religion;
- specific social status;
- medical health information;
- financial accounts;
- tracking / location information; and
- 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; and
- Ministry of Science and Technology.

It is also anticipated that the local Public Security Bureau branches and industry regulators will still have a role in both management and enforcement of data protection; and the TC260 technical committee will continue to have delegated responsibility to publish technical standards.

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 filling 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

Collection

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, separate consent (i.e. explicit 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.

In addition, the PIPL requires 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);
- protecting the interests of natural person during any public health emergency or otherwise responding to a public health emergency, or in an emergency to protect the safety of natural persons’ health and property;
- carrying out news reporting and public opinion monitoring for public interests;
- the personal information being processed is already made public legally and the processing is within the reasonable scope and in accordance with the requirements of the PIPL; 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 party processors (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;
- circumstances under which the data controller will transfer, share or assign personal information to third party controllers, the names and contact information of third party controllers, purpose and means of processing and personal information categories;
- circumstances under which the personal information will be transferred, accessed or stored outside of the PRC, the names and contact information of overseas recipients, purpose and means of processing, personal information categories and the means and procedures for individuals to exercise their data subject rights against the overseas recipients;
- 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. On March 1, 2022, the Administrative Provisions on Recommendation Algorithms in Internet-based Information Services came into effect, which require recommendation algorithm-based service providers to establish management systems and technical measures for data security and personal information protection.

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 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.

The "Guidance for Personal Information Security Impact Assessment" (PIIA Guidelines) (published by the National Standardization Technical Committee for Information Security) came into force on June 1, 2021.

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:

- if the third party is a separate data controller, inform the data subject of the purposes of the sharing, disclosure or transfer of the personal information the types of data shared, the name and contact information of the recipient, and obtain prior separate 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

Most personal information can be transferred or accessed outside of the PRC providing the following compliance steps are taken:

- the data controller has completed one of the following mechanisms to legitimize overseas data transfer, unless the transfer is exempted from such requirement — for details please see below:
  - the organisation has passed a CAC security assessment;
  - the organisation has obtained certification from a CAC-accredited agency;
  - the organisation has put in place CAC standard contractual clauses (SCCs) with the data recipient and filed the signed SCCs with the local CAC together with a cross-border transfer specific PIIA report; 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).

1. Exempted Transfers

According to the Regulations on Facilitating and Regulating the Cross–border Data Transfers, the following cross-border data transfers are exempted from having to follow any one of the legitimising mechanisms above ("Exempted Transfers”):

- Collection outside of PRC the personal information being transferred outside of PRC was originally collected and generated outside of PRC and thereafter imported back into PRC, and the processing of such personal information within PRC does not involve any personal information or important data that is collected from or generated in PRC;
- Cross-border HR management: the transfer is necessary for implementing cross-border human resource management in accordance with legally formulated employment policies and procedures or legally executed collective contracts;

- Cross-border contract: the transfer is necessary for concluding or performing a contract between the data subject and the data controller (e.g. those contracts that relate to cross-border shipping, logistics, remittance, payments, bank account opening, flight and hotel booking, visa applications, examination services etc.); or
- Emergency situation: the transfer is necessary for protecting the life, health or property security of any natural person under emergency circumstances.

Exempted Transfers 2 (cross-border HR management) and 3 (cross-border contracts) above rely on a “necessity” test. This means the organisation must prove that the cross-border data transfer is necessary in order for the exemption to apply. However, it remains unclear as to what would constitute a necessary basis for the cross-border transfer of personal information.

After carving out all the Exempted Transfers, the data controller shall determine the applicable mechanisms to legitimise the rest overseas data transfers as follows:

2. CAC security assessment

According to the Regulations on Facilitating and Regulating the Cross–border Data Transfers, a CAC security assessment is required for data controllers who meet any of the following thresholds:

- an organisation intends to transfer any "important data" overseas;
- a CIIO intends to transfer any personal information overseas;
- a data controller intends to transfer non-sensitive personal information of more than 1,000,000 individuals overseas since 1 January of the year when the calculation is conducted; or
- a data controller intends to transfer sensitive personal information of more than 10,000 individuals overseas since 1 January of the year when the calculation is conducted.

The CAC security assessment involves the organisation completing a self–assessment of its cross-border data transfers, which must then be submitted for approval by both the local and national CAC. It primarily assesses the impact of overseas transfers on national security, public interest, and the legitimate rights and interests of individuals or organisations. If the CAC security assessment is passed, the organisation will be granted with a written approval. Such approval will be valid for 3 years and could be extended for another 3 years upon approval by both the local and national CAC, provided the organisation has made no change to its previously approved cross–border transfers.

For organisations that must follow the CAC security assessment route, a copy of the data must in practice be stored locally in the PRC.

3. China SCCs

According to the Regulations on Facilitating and Regulating the Cross–border Data Transfers, a China SCCs filing with the CAC is required for data controllers who meet any of the following thresholds:

- a data controller intends to transfer non-sensitive personal information of between 100,000 and 1,000,000 individuals overseas since 1 January of the year when the calculation is conducted; or
- a data controller intends to transfer sensitive personal information of fewer than 10,000 individuals overseas since 1 January of the year when the calculation is conducted.

For PRC data controllers that must follow the China SCCs filing route, they must put in place the China SCCs with the overseas data recipient, and then within 10 working days after the effectiveness of the China SCCs file a copy of the signed SCCs together with the corresponding PIIA with the local CAC.

The Measures for the Standard Contract for the Outbound Transfer of Personal Information and the Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information (Second Edition) provide clarification on how the SCCs may be implemented by organisations as one of the mechanisms for overseas data transfer under the PIPL, how to prepare the corresponding PIIA by using the standard template formulated by the CAC and the procedures for filing the signed SCCs and the PIIA report.

4. CAC certification

The CAC certification route applies to organisations who trigger the same thresholds as the China SCCs. However, there remains uncertainty around its applicability. According to the Practicing Guidelines for Network Security Standards — Technical Specification for Certification of Personal Information Cross–border Processing Activities (V2.0), it will once implemented set up a framework of certification of overseas data transfer, including the principles, data protection obligations of data controllers and the overseas recipient, ensuring data subject rights, etc. Details to implement the certification remain unclear.

Organisations within regulated industry sectors may have to follow other compliance steps prescribed by their industry regulator to transfer or remote access their personal information outside of the PRC.

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

- 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.).

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.

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 the PRC 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 the PRC 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.

5. Transfer of personal information within the Greater Bay Area

Given the close integration of cities within the Guangdong–Hong Kong–Macao Greater Bay Area (GBA), and that data flows between Hong Kong and other cities within the GBA are becoming increasingly frequent, the CAC and the Innovation, Technology and Industry Bureau of the Government of the Hong Kong Special Administrative Region (ITIB) and Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) together formulated the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong– Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong) (GBA SCCs).

In addition to complying with other general data protection requirements (e.g. notice, consent and impact assessment, etc.) if the data controller and the data recipient are registered in Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Dongguan, Zhongshan, Jiangmen, Zhaoqing or Hong Kong SAR, they may consider signing the GBA SCCs to legitimize the transfer and file the signed GBA SCCs with the Guangdong CAC and PCPD.

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).

Industrial regulators in each sector are working on issuing the data classification scheme in the relevant sectors. In particular, the Ministry of Industry and Information Technology recently issued the Measures for Data Security Management in the Industrial and Information Technology Sector (for Trial Implementation) (MIIT Measures) which came into force on January 1, 2023. The MIIT Measures provide standards for data classification and grading scheme in the industrial and information technology sector and classify data into three grades: general data, important data, and core data. Additionally, the Draft National Standard of Information Security Technology — Requirements for Classification and Grading of Network Data provides the principles and methods for data classification and grading.

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, in particular:

1. Malicious program incidents;
2. Network attack incidents;
3. Data security incidents;
4. Information content security incidents;
5. Equipment and facility failure incidents;
6. Operational violation incidents;
7. Security risk incidents;
8. Abnormal behavior incidents;
9. Force majeure incidents; and
10. Other cyber incidents.

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 information 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. On 8 December 2023, the CAC released the Draft Administrative Measures on Cybersecurity Incident Reporting to solicit public opinions. This draft proposes new mechanisms to classify cybersecurity incidents and new reporting obligations.

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; and
- 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 the PRC'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 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 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.

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

Amanda Ge
Of Counsel
DLA Piper
T +86 185 1511 8230
amanda.ge@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.