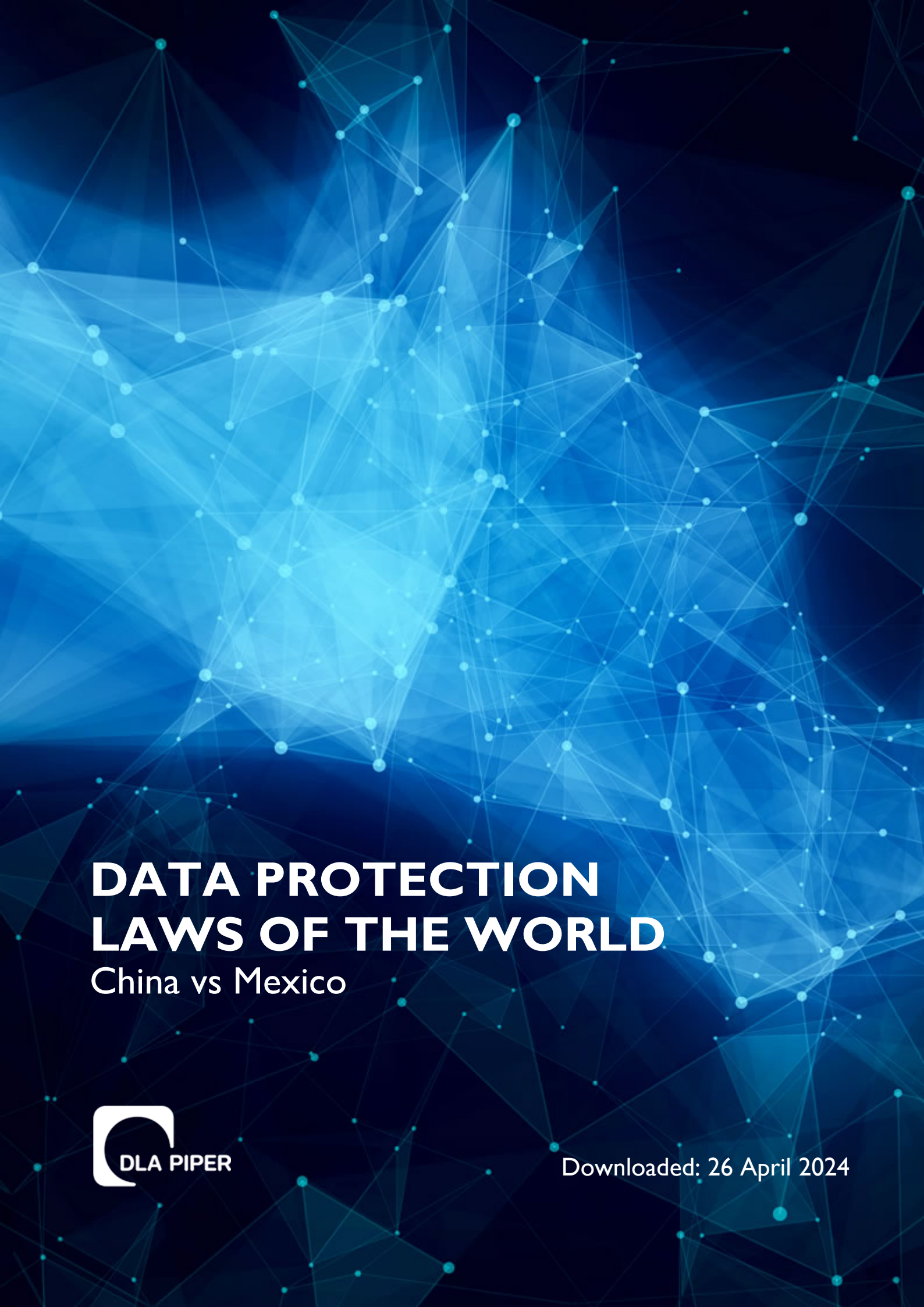

DATA PROTECTION LAWS OF THE WORLD

China vs Mexico

DLA PIPER

CHINA

Last modified 18 December 2023

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;

MEXICO

Last modified 28 January 2024

LAW

The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) ("the Law") entered into force on July 6, 2010.

Subsequently, the Executive Branch has also issued the following (collectively, with the Law, referred to herein as "Mexican Privacy Laws"):

- The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (the Regulations), which entered into force on December 22, 2011
- The Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013
- The Recommendations on Personal Data Security, on November 30, 2013
- The Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014
- The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), which entered into force on January 27, 2017

On June 12, 2018, a decree was published in the Official Gazette of the Federation approving two important documents:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981, and its
- Additional Protocol regarding supervisory authorities and trans-border data flows dated November 8, 2001.

Mexican Privacy Laws apply to all personal data processing under any of the following circumstances:

- The Measures for the Security Assessment of Outbound Data Transfers, effective from September 1, 2022; and
- The Measures for the Standard Contract for the Outbound Transfer of Personal Information, effective from 1 June 2023.

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;
- Guidelines on Application of Security Assessment of Cross-border Data Transfers (First Version), effective from 1 September, 2022;
- 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;
- Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information (First Edition), effective from 1 June 2023; and
- 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.

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

- Processing carried out by a data controller established in Mexican territory
- Processing carried out by a data processor, regardless of its location, if the processing is performed on behalf of a data controller established in Mexico
- Processing by or on behalf of a data controller not located in Mexico, where Mexican legislation is applicable pursuant to the execution of an agreement or Mexico’s adherence to an international convention or
- Processing carried out within Mexican territory, on behalf of a data controller not established in Mexican territory, unless such processing is only for transit purposes

The Law only applies to private individuals or legal entities that process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or persons carrying out the collection and storage of personal data exclusively for personal use where it is not disclosed for commercial use. Further, Mexican Privacy Law also does not generally apply to business-to-business data, including:

- Data of legal entities.
- Data of individuals acting as merchants or professionals.
- Data of natural persons acting on behalf of a business (e.g., their employer), where the personal data processed is (a) limited to first and last names, title, position and functions performed, and business contact data, such as mailing or physical address, email address, telephone number and fax number, and (b) the personal data is processed solely for the purpose of representing the business or administering the business relationship (i.e., fulfilling orders, providing services, carrying out transactions between the business entities)

Additionally, the INAI has issued several documents and guidelines for the private sector regarding the processing of personal data, including the following:

- The Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013
- The Recommendations on Personal Data Security, on November 30, 2013
- The Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014

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.

- Recommendations for the Designation of the Data Protection Officer or the Data Protection Department
- Guideline to Implement Compensatory Measures
- Guideline for the orientation of the due processing of personal data in the activity of extrajudicial collection
- Guideline for the Secure Deletion of Personal Data
- Suggested minimum criteria for contracting cloud computing services that involve the processing of personal data
- Guideline for the Processing of Biometric Data.

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): (i) biometric data; (ii) religion; (iii) specific social status; (iv) medical health information; (v) financial accounts; (vi) tracking / location information; and (vii) minors’ data.

DEFINITIONS

Definition of personal data

‘Personal data’ is any information concerning an identified or identifiable individual.

Definition of sensitive personal data

‘Sensitive personal data’ is personal data that affects the most intimate areas of the data subject’s life, which if misused, may lead to discrimination or entail a serious risk to the data subject. In particular, the definition includes data that may reveal any of the following:

- Racial or ethnic origin
- Past or present health conditions
- Genetic information
- Religious, philosophical or moral beliefs
- Union affiliation
- Political views
- Sexual orientation
- Pictures and videos
- Fingerprints
- Geolocation
- Banking information
- Signature

Other key definitions

'ARCO Rights' refer to the access, ratification, cancelation and opposition rights of data subjects, with respect to their personal data.

'Controller' or 'data controller' means the individual or private entity makes decisions regarding the processing of personal data.

'Data subject' means the individual to which the personal data belongs.

'Guidelines' means the guidelines issued by INAI, regarding the compliance with the principles and duties of the Data Privacy Law.

'INAI' refers to the National Institute of Transparency, Access to Information and Protection of Personal Data (***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales***).

'Privacy notice' means the physical or electronic document, or document generated in any other form by the controller and made available to data subjects, prior to the processing of their personal data. There are three forms of a privacy notice: comprehensive or full-form, simplified, and short.

'Processing' means any collection, use, disclosure or storage of personal data made through any means, including any access, handling, exploitation, transfer or disposal of personal data.

'Processor' or 'data processor' means the individual or entity that separately or jointly with others processes personal data on behalf of the controller.

'Remittance' any communication of personal data carried out between the controller and the processor, within or outside Mexican territory.

'Third Party' means an individual or entity, whether national or foreigner, that is not the data subject, the controller or the processor of the personal data.

'Transfer' means any communication of personal data carried out between the controller and any third party.

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

NATIONAL DATA PROTECTION AUTHORITY

The National Institute of Transparency for Access to Information and Personal Data Protection (***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales***) (INAI) and the Ministry of Economy (Secretaría de Economía) serve as Mexico’s data protection authorities.

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

REGISTRATION

Mexican law does not require registration with a data protection authority or other regulator in relation to the use of personal data.

DATA PROTECTION OFFICERS

All data controllers are required to designate a personal data officer or department (each, a Data Protection Officer) to handle requests from data subjects exercising their ARCO Rights (as defined in ‘Collection and Processing’) under the Law. Data Protection Officers are also responsible for overseeing and advising on the protection of personal data within their organizations.

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

Principles and obligations

In processing personal data, data controllers must observe the principles of legality, information, consent, notice, quality, purpose, loyalty, proportionality and accountability.

Pursuant to these principles:

- Personal data must be collected and processed fairly (and not through deceptive or fraudulent means) and lawfully
- Personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes.
- Consent must be obtained, unless an exception applies.
- Processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected. or further processed
- Personal data must be accurate and, if necessary, updated; every reasonable step must be taken to ensure that data that is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified., and
- Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.
- Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data. In addition, personal data must be processed as agreed upon by the parties (in a privacy notice or otherwise) and in compliance with the Law.
- A privacy notice (Aviso de Privacidad) must be made available to data subjects prior to the processing of their personal data.

Required information for privacy notices

To legally process personal data, data controllers must provide a privacy notice (Aviso de Privacidad), which must be made available to a data subject prior to the processing of his or her personal data. The privacy notice may be provided to data subjects in printed, digital, visual or audio formats, or any other technology.

Controllers are required to notify data subjects of the main characteristics of the processing to which their personal data will be subject. This obligation is complied

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;

with through the privacy notice. Therefore, any data controller is required to prepare and make available to data subjects the relevant privacy notice(s) corresponding to their personal data. Controllers will have to make available distinct privacy notices for different categories of data subjects, such as personnel and customers.

The Guidelines permit the following three forms of privacy notice, depending on whether the personal data is obtained directly or indirectly from the data subject, and the context and space in which the personal data is collected:

- **Comprehensive privacy notice**: required to be provided when the personal data is obtained in-person from the data subject, for example, in a face-to-face interview.
- **Simplified privacy notice**: required to be provided when the data is obtained directly from the data subject, for example, when registering for an account on website or during a customer service call.
- **Short form privacy notice**: may be provided when the space for the privacy notice is limited and the Personal Data collected is minimum, for example, at an ATM, in a SMS, on a raffle ticket

Each of these forms must meet specific disclosure requirements, as described below, and the simplified and short-form notices must link to, or provide information about how to obtain, the comprehensive notice.

A **comprehensive privacy notice** must at least contain:

- The identity and address of the data controller
- A description of the personal data that will be processed
- Identification of any sensitive personal data that will be processed, and an affirmative statement that such data will be processed (if applicable)
- The purposes of the data processing, including the primary and any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes
- The means by which data subjects can revoke their consent
- The means for exercising rights of access, rectification, cancellation or objection (ARCO rights)
- Where appropriate, the types of data transfers to be made, including the purposes of such transfers and the identification of any third parties (not

- circumstances under which the personal information will be transferred, accessed or stored outside of the PRC, the names and contact information of overseas recipi-ents, 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

including processors) to whom personal data is transferred
- The procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice, and Identification of any sensitive personal data that will be processed

A **simplified privacy notice** must include, at least, the following information:

- The identity and address of the Controller
- The purposes of the data processing, including the primary and any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes
- How to access or obtain the comprehensive privacy notice

The **short form privacy notice** must include, at least, the following information:

- The identity and address of the Controller
- The purposes of the data processing, without distinguishing any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes

In addition to the required information, a privacy notice must be clear and in a comprehensible language, and with an easy structure and design, which means it should among other things, the privacy notice should not use inappropriate, ambiguous, or vague sentences, or refer to texts and documents that are not available for the data subject to review.

The data controller has the burden of proof to show that the privacy notice was provided to the data subjects prior to the processing of their personal data (unless an exception applies). However, controllers are not required to provide a privacy notice where:

- personal data is obtained indirectly and it is intended for historical, statistical, or scientific purposes
- where the personal data collected is not subject to Mexican Privacy Laws (*eg*, certain business-to-business data as described previously)

Consent to processing

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.

Except as otherwise provided by the Law, some form of consent is required for all processing of personal data; depending upon the circumstances consent may be implicit, express, or express and written:

Implicit (or tacit) consent applies to the processing of personal data generally, except where the Law requires express or express written consent (or where consent is not required):

- Implicit consent is obtained where the data subject has been informed of the privacy notice and has not objected to or refused the processing of personal data as described in the privacy notice.
- Express consent (notice and opt-in) is required for o the processing of financial or asset data.
- Express consent may be obtained verbally, in writing, or via any technology or other unmistakable indication. Express and written consent is required for the processing of sensitive personal data. Express written consent may be obtained through the data subject’s written signature, electronic signature, or any other authentication mechanism.

In addition to the above, express or express written consent must be obtained where otherwise specifically required pursuant to an applicable law.

On the other hand, consent from the data subject is not required (but a privacy notice must still be made available) for the processing of personal data where any of the following apply:

- The processing is required pursuant to an applicable Mexican law
- The data is contained in publicly available sources
- The identity of the data subject has been disassociated from the data (*ie*, the data subject is no longer identifiable)
- Where the processing is for the purpose of fulfilling obligations pursuant to a legal relationship between the data subject and the data controller
- There is an emergency situation that could potentially harm an individual with regard to his or her person or property
- Processing is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the manner established by the General Health Law (Ley General de Salud) and

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 — for details please see below:

TRANSFER

Mexican privacy laws distinguish between 'transfers' of personal data (to third parties) and transmissions of personal data (to processors). Under Mexican Privacy Laws, a 'transfer' is any communication or transmission of personal data by or on behalf of the Controller to a third party (not including a processor). Where the data controller intends to transfer personal data to domestic or foreign third parties other than a data processor, it must provide the third parties with the privacy notice provided to the data subject and the purposes to which the data subject has limited the data processing. In addition, the controller must notify data subjects in the privacy notice of the transfer, including:

- that the transfer may be made, as well as to whom and for what purposes the personal data may be transferred.
- where consent to the transfer is required, that the data subject consents and how the data subject can refuse to consent to the relevant transfer(s).

The purpose of the transfer must be limited to the purpose and conditions informed in the privacy notice and consented to by the data subject (as applicable).

The third-party recipient must assume the same obligations as the data controller who has transferred the data.

Domestic and international transfers of personal data may be carried out without the consent of the data subject where the transfer is:

- Pursuant to a law or treaty to which Mexico is party
- Necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management
- Made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal other applicable laws, and said processing is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or
- Pursuant to a resolution issued by a competent authority

    - 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).

In terms of the mechanisms to legitimise overseas data transfer referred to above:

1. CAC security assessment

According to the Measures for the Security Assessment of 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 which processes personal information of more than 1,000,000 individuals and intends to transfer personal information overseas; or
- a data controller who in aggregate transfers overseas personal information of more than 100,000 individuals, or sensitive personal information of more than 10,000 individuals since 1 January of the preceding year.

The CAC security assessment involves the organisation completing a self–assessment of its cross-border data transfers, which must then be submitted for approval

processes and policies as the data controller (provided they will comply with principles of Mexican Privacy Laws, the privacy notice provided to data subjects and the other applicable internal policies regarding data protection)
- Necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject
- Necessary or legally required to safeguard public interest or for the administration of justice
- Necessary for the recognition, exercise or defense of a right in a judicial proceeding, or
- Necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject

The Regulations establish that communications or transmissions of personal data to processors do not need to be notified or consented to by the data subject. However, the data processor must do all of the following:

- Process personal data only according to the instructions of the data controller
- Not process personal data for a purpose other than as instructed by the data controller
- Implement the security measures required by the Law, the Regulations and other applicable laws and regulations
- Maintain the confidentiality of the personal data subject to processing
- Delete personal data that were processed after the legal relationship with the data controller ends or when instructed by the data controller, unless there is a legal requirement for the preservation of the personal data
- Not transfer personal data unless instructed by the data controller, the communication arises from subcontracting, or if so required by a competent authority

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 should be renewed every two years, or updated if there are changes to the 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.

2. China SCCs

For PRC data controllers that do not meet the threshold for the CAC security assessment, 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 with the local CAC branch together with the corresponding PIIA.

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 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.

3. CAC certification

The CAC certification route applies to organisations not caught by the CAC security assessment or SCCs route, and appears largely in practice to catch non-PRC data controllers who do not meet the CAC security assessment threshold. 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 data) 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.

4. 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

SECURITY

All data controllers must establish and maintain physical, technical and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. They may not adopt security measures that are inferior to those they have in place to manage their own information.

The risk involved, potential consequences for the data subjects, sensitivity of the data and technological development must be taken into account when establishing security measures, and more care should be taken in the collection and process of sensitive personal data.

The Controller also has the obligation to train its personnel on the proper handling of personal data in order to ensure compliance with the Mexican Privacy Laws. Per the Guidelines, a controller must also establish, document and follow security policies and procedures, including:

- Maintaining an inventory of personal data and the relevant processing systems, and update this at least once per year with respect to sensitive personal data
- Identifying the duties and obligations of persons that processing personal data on behalf of the controller
- Conducting appropriate risk analyses to identify dangers and estimate risk of harm to personal data
- Establishing security measures applicable and confirm they are effectively implemented
- Assessing and improving security on an ongoing basis
- Establishing a roadmap to implement any missing security measures identified pursuant to a security breach (as necessary to prevent a recurrence of such breach)
- Performing reviews or audits of security program

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.

- Maintaining records of the storage means for personal data

BREACH NOTIFICATION

Security breaches occurring at any stage of the processing that materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject.

Under Mexican Privacy Laws, a security breach of personal data includes any unauthorized:

- loss or destruction of personal data
- theft, loss or copying of personal data
- use, access or processing of personal data
- damage or alteration of personal data

If there is a breach of personal data, the controller must first analyze the causes of such breach; and then take

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 steps to implement any corrective, preventive, improvement actions necessary to prevent the breach from recurring.

If a breach significantly affects the property or moral rights of the data subjects, the controller must immediately notify the affected data subjects, as soon as it confirms that the breach has occurred, so that the affected Data Subjects can take the corresponding measures.

The Regulations provide that breach notification must include at least the following information:

- The nature of the breach
- The personal data compromised
- Recommendations to the data subject concerning measures that he or she can adopt to protect his or her interests
- Immediate corrective actions implemented in response to the breach, and
- The means by which the data subject may obtain more information in regard to the data breach

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.

ENFORCEMENT

Data subjects can enforce their ARCO Rights, when no response is obtained from the data controller via INAI and ultimately the court system.

If any breach of the Law or its Regulations is alleged, INAI may perform an on-site inspection at the data controller’s facilities to verify compliance with the Law.

Violations of the Law may result in monetary penalties or imprisonment, including the following:

INAI may impose monetary sanctions in the range of 100 to 320,000 times the Mexico City minimum wage (currently, MX $88.36, updated every year). Sanctions may be increased up to double the above amounts for violations involving sensitive personal data.

Three months to three years of imprisonment may be imposed on any person authorized to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if sensitive personal data is involved.

Six months to five years of imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorized to process such data. Penalties will be doubled if sensitive personal data is involved.

In determining the appropriate sanctions, the INAI will consider:

- The nature of the data
- The notorious inadmissibility of the refusal of the Data Controller, to carry out the acts requested by the data subject, in terms of this Law

- The intentional or unintentional nature of the action or omission constituting the offense
- The economic capacity of the data controller, and
- Recidivism

The sanctions imposed by the INAI are without prejudice to any further civil or criminal liability.

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.

ELECTRONIC MARKETING

Email marketing constitutes personal data processing and is subject to the Law, including applicable notice and consent requirements.

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;

ONLINE PRIVACY

The Regulations and Guidelines that address the use of cookies, web beacons and other analogous technologies, require that when a data controller uses online tracking mechanisms that permit the automatic collection of personal data, it provides prominent notice of the use of such technologies; the fact that personal data is being collected the type of personal data collected and the purpose of the collection and the options to disable such technologies.

An IP address alone may be considered personal data, however, there has not been a resolution or decision issued by the competent authority on this point.

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.

KEY CONTACTS

Gabriela Alaña
Partner
T + 52 55 5261.1817
gabriela.alana@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.