Baker McKenzie FenXun. 奋迅·贝克麦坚时

Client Alert

August 2021

China established a comprehensive personal information protection regime

Executive Summary

On 20 August 2021, the Standing Committee of the National People's Congress passed the Personal Information Protection Law of the PRC (PIPL), after deliberating two draft versions and seeking public comment in a ten-month span. **The passage of the PIPL signifies that China is stepping into a more robust and comprehensive personal information protection regime by establishing a unified, cross-sector legislation**, as the EU does with the aid of the General Data Protection Regulation ("**GDPR**").

Contents

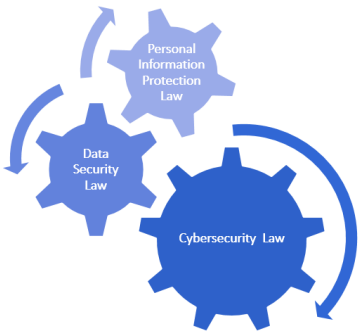
The PIPL, in general, establishes a regime similar to the GDPR, although the requirements may not be entirely the same, with the PIPL imposing stricter requirements in some areas. For instance, the PIPL imposes **heightened requirements in terms of details to be disclosed to individuals for processing of sensitive personal information and cross-border provision of personal information** (pursuant to the PIPL, the name and contact details of each and every foreign recipient must be disclosed), and requires **separate consent** from individuals to the same. Also, the PIPL **mandates controllers to conduct security impact assessments for under a number of processing scenarios**. Further, the PIPL imposes a **data localization requirement** on operators of critical information infrastructure and controllers that process an over-the-threshold volume of personal information (the threshold will likely be set at one million personal information subjects). In addition, the PIPL **exerts more rigid control over cross-border data transfers**.

Being GDPR-compliant does not warrant being PIPL-compliant. Companies are advised to take actions as soon as practically feasible to ensure that their China-related privacy practices are compliant with the requirements prescribed under the PIPL, as the PIPL will soon **take effect from 1 November 2021**. We recommend that companies:

- Develop a data governance framework and an in-house data compliance program.
- Conduct data mapping and data inventory check, system profiling as well as security risk identification and profiling.
- Review and update existing privacy notices that apply to Chinese residents by measuring against the requirements (especially taking into account the heightened notification and separate consent requirements) under the PIPL.
- Develop and update internal policies, protocols, standard operating procedures, and response mechanisms in regard to protection of personal information, including, **among others**, conducting security impact assessments and establishing a channel of responding to requests of personal information subjects.
- Review and prepare for data localization to the extent applicable.
- Review and prepare for cross-border data transfers, restrictions and formalities.
- Maintain and document appropriate contractual, technical, organizational and physical privacy and security measures for China, including the performance of due diligence of vendors, the management of vendor agreements, the monitoring of vendor compliance, and the administration of regular data privacy and security training for personnel.

With the enactment of the PIPL, **the Chinese legislature has promulgated all of the "Three Horse Carriages" for data protection and cybersecurity regimes of the new age**, namely: (i) the **Cybersecurity Law of the PRC**, governing the construction, operation, maintenance, use and security of (cyber) network in the PRC territory; (ii) the **Data Security Law of the PRC**, principally dealing with data security, governance and trading, with a focus on data other than personal information; and (iii) the **PIPL**, which regulates personal information and related matters. Going forward, cybersecurity, non-personally-identifiable data and personal information will be regulated under these three principal laws separately.

"Three Horse Carriages" for Personal Information Protection Regime



In-depth Overview

This article aims to walk you through the most critical requirements contained in the PIPL that may be relevant to your China-related business operations.[1]

In this article, the terms "**China**" and "**PRC**" refer to mainland of the People's Republic of China, excluding the Hong Kong and Macau Special Administrative Regions and Taiwan, which Chinese personal information protection regime regards as foreign jurisdictions. The term "**Chinese**" refers to China only. The term "**foreign**" or "**overseas**" should be read accordingly.

1. What is regarded as personal information and sensitive personal information?

Personal information means all types of information relating to an identified or identifiable natural person.

The PIPL defines personal information as all types of information, whether recorded in electronic or other formats, **relating to an identified or identifiable natural person**, excluding anonymized information. This definition is similar to the GDPR, while the GDPR does not define the term in relation to any particular format.

By resorting to the *Personal Information Security Specification* (GB/T 35273-2020) ("**Specification**"), an important and frequently-quoted national standard with recommended effect, one may follow two approaches in determining whether a specific piece of information should be regarded as personal information: (i) whether the information can be used to identify an individual through the specificities, peculiarities and features of the information concerned (such as identity related information, biometric information); and (ii) whether the information is associated with an individual, *e.g.* the information generated in the course of the activities of a known natural person (such as location tracks, web browsing logs). According to the Specification, any information that meets either of the two criteria above should be categorized as personal information.

As one can tell, personal information in the Chinese law context is intended to be defined and delineated in a rather broad fashion, and with such board definition, **the exact scope of personal information would be dynamic and depends greatly on the exact context, scenario and use case in question**.

It is also worthy of note that Chinese personal information protection rules do not make a distinction between business contact information and personal contact information as some of the other jurisdictions may do, and therefore, business contact information that is collected and processed in a B2B context (*e.g.* contact person's name, position or title, business landline and telephone number, business email address) will unexceptionally fall into the parameters of the broadly-delineated personal information under Chinese law.

Another concept—"**sensitive personal information**"—is defined by the PIPL as personal information that, once divulged or illegally used, may easily cause harm to the dignity of natural persons or endanger personal or property safety. Examples given in the law include **biometric, religious belief, specific identity, medical and health care, financial account, location tracks and other information, as well as personal information of minors under the age of 14**. From a PIPL-compliant standpoint, how to scope sensitive personal information is of great importance, as the PIPL imposes special rules in regard to the processing of sensitive personal information, as elaborated below.

[1] This article intentionally disregards the requirements that are specifically applicable to Chinese government agencies.

2. What types of processing are regulated?

Similar to the GDPR, the PIPL defines "**processing**" as **collection, storage, use, processing, transmission, provision, public disclosure, deletion and any operation which is performed on personal information**. Under this broad definition, all types of processing throughout the lifecycle of personal information will be covered, and thus, regulated.

3. Which government organs take charge of personal information protection in China?

The Cyberspace Administration of China ("**CAC**"), pursuant to the PIPL, will be the authority in charge of the overall planning and coordination of the protection of personal information and relevant regulatory affairs. Aside from the CAC, sectorial regulators are and will continue to be responsible for overseeing and enforcing various personal information protection requirements within their respective purview. The CAC and sectorial regulators are collectively referred to as "**Chinese personal information protection authorities**".

4. In what ways does the PIPL distinguish between controllers and processors?

The PIPL creates a distinction between controllers and processors, although it adopts different naming conventions for the same. Specifically, the PIPL establishes a term "personal information processor" or "**PIP**" and defines it as an organization or individual that independently determines the purposes and means of the processing of personal information in the course of personal information processing activities. This concept is akin to the controller promulgated in the GDPR.

The PIPL also establishes a concept similar to joint controllers under the GDPR.

The PIPL adopts the term "**entrusted person**" and provides that a PIP may entrust a person to process personal information on its behalf with the PIP still being responsible for compliance with the majority of personal information processing obligations under the PIPL. Such concept is similar to the processor stipulated in the GDPR.

5. How the PIPL applies extra-territorially to organizations or individuals outside of the country? Will foreign PIP (*i.e.* controllers) have to appoint a local representative in China?

The PIPL and other Chinese personal information protection rules aim to protect personal information of natural persons residing in China (hereinafter referred to as "**Chinese residents**" for convenience).

Aside from the domestic jurisdiction, China is expanding the geographic scope of application of its personal information protection regime, by empowering that **the PIPL applies to processing activities conducted outside of the PRC involving personal information of Chinese residents where the processing activities: (i) are for the purpose of offering products or services to individuals in China; (ii) analyze and evaluate the behavior of individuals in China**; or (iii) meet other circumstances provided under the laws or administrative regulations. Circumstances (i) and (ii) above closely parallel those in which the GDPR provides that it has extra-territorial effect.

> The PIPL applies to foreign controllers to the extent of their processing of personal information of Chinese residents, where the processing activities:
>
> - are for the purpose of offering products or services to individuals in China; or
> - analyze and evaluate the behavior of individuals in China.

Pursuant to the PIPL, **a foreign PIP that is subject to extra-territorial application of the PIPL should establish a dedicated local organization or representative in China**, similar to the requirement in the GDPR except that the requirement only applies to PIPs. The local organization or representative will be responsible for handling the relevant affairs concerning the protection of personal information of Chinese residents, and the foreign PIP must report the local organization or representative's name and contact details to Chinese personal information protection authorities. This requirement is stricter than the GDPR, which only demands the representative's contact details to be included in privacy notices. We anticipate further clarification from the CAC as to (i) the reporting procedure (whether it will be structured as a recordal or even more procedurally-light process), and (ii) whether the local organization or representative could be penalized merely as a result of the foreign PIP contravening Chinese personal information protection requirements.

6. Who bears the obligations to comply with the PIPL? Will obligations differ based on the volume of personal information processed? Who must store personal information locally in China?

The PIPL applies to all sectors, all types of organizations (including government agencies) and all processing activities except for (i) processing of personal information by PRC government agencies when carrying out statistical or records or archives management

activities, which may be governed by special sets of rules, and (ii) the processing of personal information by an individual for personal or family reasons.

On the face of the PIPL, PIPs are subject to virtually all of the personal information protection requirements, while entrusted persons who process personal information on the behalf of PIPs should take necessary measures to protect security of personal information processed and "*assist*" with PIPs to fulfil their obligations under the law.

Pursuant to the PIPL, the level of obligations can differ among PIPs based on the volume of personal information that they process.

(a) **Operators of critical information infrastructure** ("**CII**") and **PIPs that process personal information above certain prescribed volume (likely to be 1 million personal information subjects)** will be subject to heightened obligations, *e.g.* they are obligated to (i) **store in China personal information collected and generated in the PRC territory** and (ii) **pass the CAC-administered security assessment before such personal information can be exported overseas**, unless the laws, administrative regulations and CAC's rules otherwise provide that security assessment is not needed.

The data localization requirement applies to (i) operators of critical information infrastructure and (ii) controllers who process an over-the-threshold volume of personal information (so far, likely be 1 million personal information subjects as threshold).

The CII is defined as the important network facilities and information systems, etc. in important industries and sectors such as **public telecommunications and information services, energy, transportation, water conservancy, finance, public services, e-government, and national defense science and technology industry**, as well as other important network facilities and information systems, etc. that, if destroyed, disabled, or suffering a data leak, would **seriously endanger the State security, national welfare, the people's livelihood, and public interests**. Such definition is provided in the *Regulations on the Security Protection of Critical Information Infrastructure* recently promulgated on 30 July 2021, pursuant to which, sectorial regulators will formulate rules for identifying the CIIs among the sector concerned.

The PIPL does not specify the figures for thresholds in regard to the volume of personal information processed, which, once surpassed, PIPs will be subject to the same data localization and CAC-administered security assessment requirements as CII operators. Based on some previously-issued draft rules and judicial interpretations, our speculation is that **the threshold may be 1 million personal information subjects**.

(b) PIPs that provide important **Internet platform services**, have a very large number of users, and have a complex mixture of business operations will be shouldered with specific obligations, including to:

(i) establish and improve a system of compliance concerning the protection of personal information, and establish an independent organization, comprised chiefly of external members, to supervise the protection of personal information;

(ii) formulate platform rules in accordance with the principles of transparency, fairness and impartiality, which shall specify rules for the processing of personal information by the providers of goods or services on the platform and for their personal information protection obligations;

(iii) cease to provide services to product or information providers on the platform that materially violate laws or administrative regulations in their processing of personal information; and

(iv) regularly publish social responsibility reports on their protection of personal information and accept supervision by the public.

(c) Interestingly, the last-minute changes absorbed by the PIPL include, *among others*, that the CAC will publish dedicated rules and standards that apply to **small-sized PIPs**. One reading of such rule suggests that small-sized PIPs may be subject to a more lenient set of rules and standards than those promulgated in the PIPL.

7. What are key principles of processing established under the PIPL?

The PIPL establishes the following key principles in regard to processing personal information:

- Legitimacy, fairness, necessity and good faith: Processing personal information should follow the legitimacy, fairness, necessity and good faith principles, and it is not allowed to use misleading, fraudulent or coercive means to process personal information.
- Purpose limitation: Personal information must be collected for specific, reasonable purposes, be directly relevant to the purposes of processing, and be processed in a way of having the least impact on the rights and interests of individuals. In

cases where a PIP intends to process personal information for additional or different purposes, it may only proceed with the concerned individuals' fresh consent.

- Data minimization: The PIP must collect and process personal information to the minimum extent relevant and necessary to achieve the intended purposes for processing.
- Openness and transparency: A compliant privacy notice containing the requisite information must be published for individuals to review and access.
- Integrity and accuracy: The PIP must ensure the quality of personal information and refrain from causing adverse impact on the rights and interests of individuals due to inaccurate or incomplete personal information.

8. What legal basis are acknowledged under the PIPL to process personal information?

The pursuit of legitimate interests is not an acknowledged legal basis for processing under the PIPL.

The PIPL, superseding previous sole consent-based regime, establishes both consent and non-consent legal grounds for processing personal information. Under the law, a PIP is permitted to process personal information *only if*:

(a) Informed consent from the personal information subject has been obtained;

(b) Where it is required to conclude and perform a contract to which the personal information subject is a party;

(c) Where it is required to perform statutory obligations or legal duties;

(d) Where it is required to respond to public health emergencies, or protect the life, health and property safety of natural persons in emergencies;

(e) Where personal information is processed to a reasonable extent for the purposes of news report, public opinion supervision and other acts for public interest;

(f) Where personal information has already been made public by the personal information subject or through other legitimate channels, and processing of such personal information is conducted pursuant to the PIPL and to a reasonable extent; or

(g) Other circumstances provided in the laws and administrative regulations.

These legal basis of processing resemble those enumerated under the GDPR except that the GDPR also includes the pursuit of legitimate interests, which controllers in the EU rely on in many circumstances, whereas the PIPL does not.

In regard to the form of consent, the PIPL requires **consent to be given on an informed basis**, meaning that individuals are only able to give their legally effective and binding consent after being duly informed of the details outlined in Section 9. Where individuals are minors below the age of 14, consent form their legal guardian is required. **In the event of the processing of sensitive personal information, cross-border provision of personal information, provision of personal information to another PIP, or public disclosure of personal information, separate consent is mandatory**; in this regard, while the PIPL is not entirely clear, our speculation is that a separate check box or consent form is needed to secure "separate consent."

9. What information needs to be included in a privacy notice?

The PIPL requires a PIP to truthfully, accurately and completely inform individuals of the following information (usually by way of a privacy notice) in an easily noticeable way, in clear and easily comprehensible language (at least in Chinese), and **before collecting and processing personal information**[2]:

(a) The name and contact details of the PIP;

(b) The purposes and means of processing;

[2] But if, in order to protect the life, health or property of individuals in an emergency, the PIP is not able to timely inform individuals of the processing of their personal information, the PIP does not have to provide advance notice but must inform them thereof after the emergency is resolved.

(c) The s types of personal information to be processed;

(d) The period for which personal information will be stored;

(e) The way and procedure in which individuals can exercise their rights pertaining to personal information under the PIPL; and

(f) Any other information required by laws and administrative regulations.

Additional details must be included in the privacy notice if the PIP will process sensitive personal information, provide personal information to another PIP, or export personal information.

The PIP is obligated to serve such a privacy notice containing the above details, regardless of whether personal information is processed based on consent and whether personal information is collected from individuals or from other sources, unless the processing is required by law to be kept confidential or notification is otherwise not required (*e.g.* in the event of governmental surveillance and investigation).

10. What are special rules that apply to processing of sensitive personal information?

- Sufficient necessity and protection measures: The processing of sensitive personal information is permissible *only if* strict protection measures are put in place and there is sufficient necessity to justify the processing.
- Informing additional information: A PIP that seeks to process sensitive personal information will have to inform individuals specifically of (i) **the necessity of processing** and (ii) **the impacts of processing on the rights and interests of individuals**, unless the processing is required by law to be kept confidential or notification is otherwise not required.
- Obtaining separate consent: The processing of sensitive personal information requires **separate consent** from individuals, and where laws and administrative regulations so provide, written consent must be obtained and documented.
- Conducting security impact assessment: The PIP will need to conduct personal information protection **security impact assessment** before it may process sensitive personal information. A recommended national standard - *i.e. Guidance for Personal Information Security Impact Assessment* (GB/T 39335-2020) ("**SIA Guidance**") - was issued for illustration in regard to the conducting of security impact assessments.

11. What are special rules that apply to provision of personal information to another PIP?

- Informing additional information: A PIP intending to provide personal information to another PIP will need to additionally inform data subjects of (i) **the name and contact details of the third-party PIP**, (ii) the purposes and means of processing and provision of personal information, and (iii) the types of personal information to be provided and shared.
- Obtaining separate consent: **Separate consent** from individuals specifically to the provision of personal information to another PIP is required.
- Conducting security impact assessment: Before a PIP may entrust a third party to process personal information on its behalf, provide personal information to another PIP, export personal information and disclose personal information to the public, *among other scenarios*, the PIP will need to conduct a personal information protection **security impact assessment**, more specifically pursuant to the SIA Guidance.

12. What are special rules that apply to cross-border provision of personal information?

Pursuant to the PIPL, the name and contact details of each and every foreign recipient of personal information must be informed to individuals in the privacy notice.

- Informing additional information: A PIP intending to export personal information overseas (regardless of whether the foreign recipient is acting as a PIP (controller) or entrusted person (processor)) will need to additionally inform data subjects of (i) **the name and contact details of the foreign recipient**, (ii) the purposes and means of processing and cross-border provision of personal information, (iii) the types of personal information to be provided overseas, and (iv) **the way and channel made available by the foreign recipient to Chinese residents for exercising their rights**.
- Obtaining separate consent: **Separate consent** from individuals specifically to the cross-border provision of personal information is mandated.

- Conditions and restrictions regarding outbound provision of personal information: The PIPL requires that outbound provision of personal information must be for genuine business needs, the exporting PIP should ensure the processing of personal information by the foreign recipient to meet a level of personal information protection standards not inferior than those promulgated in the PIPL, and at least one of the following conditions is satisfied (to the extent applicable):
    - **CII operators and PIPs processing an aggregate volume of personal information that surpasses certain thresholds** will generally be required to undergo and pass (as clearance) **CAC-administered security assessment** as a prerequisite to being permitted to export personal information of Chinese residents (that is collected and generated in the PRC territory) overseas.
    - **PIPs may have to obtain a personal information protection certification from an eligible institution in accordance with the CAC's regulations** (to be issued). Details of the circumstances triggering certification, the certification requirements, and the scope of qualified certifying institutions are currently unclear and require further clarification. This prong is distinguished from the GDPR, which, while provides for the establishment of data protection certification mechanisms, sets certification as voluntary (as opposed to mandatory) for cross-border transfers of personal data.
    - **PIPs likely have to enter into a legally compliant contract with the foreign recipient concerning the export of personal information in accordance with standard contract to be issued by CAC**. This prong differs from the standard contractual clauses recently published by the EU in June 2021, which provide for four scenarios of cross-border transfers of personal data encompassing controller-to-controller, controller-to-processor, processor-to-controller, and processor-to-processor. But on the face of the PIPL, the obligation to enter into a data export agreement seems to solely lie on the PIP (but not entrusted persons *i.e.* processors), and therefore, the scenarios being captured might only cover controller-to-controller and controller-to-processor transfers. We anticipate that the CAC could provide more clarification in this juncture through the to-be-issued standard contract or contractual clauses.

Conditions for cross-border provision of personal information - at least meet one:

- Passing CAC-administered security review
- Obtaining a personal information protection certification;
- Entering into a data export agreement that is compliant with CAC's standard contract (to be issued).

- Conducting security impact assessment: The PIP exporting personal information will need to perform a personal information protection **security impact assessment**, more specifically pursuant to the SIA Guidance.

13. What rights may personal information subjects exercise?

The PIPL gives individuals a broad suite of rights pertaining to their personal information, as the GDPR does. In particular, the law would permit individuals[3] to:

- **Know about and decide on the processing of their personal information**, including to restrict or refuse the processing of their personal information, unless otherwise provide by laws and administrative regulations;
- **Access and make copies of their personal information**, unless the processing is required by law to be kept confidential or notification is otherwise not required;
- Request that a PIP transfer their personal information to another PIP designated by them (this is equivalent to the **right of data portability** provided under the GDPR);
- Request that a PIP update or supplement their personal information if it is inaccurate or incomplete;
- Request to **withdraw consent with future effect**, where personal information is processed based on their consent;
- Request that their personal information be deleted where:

The PIPL, for the first time, acknowledges the right of data portability.

[3] In the event of the death of an individual, the rights pertaining to personal information of the deceased may be exercised by his or her close relatives for their own legitimate and rightful interests, unless the deceased made other arrangements during his or her lifetime.

- the purposes of processing have been achieved or cannot be achieved, or if such personal information is no longer required to achieve such purpose;
- the PIP has ceased to offer the products or services, or the retention period has expired;
- individuals have withdrawn their consent and the processing is based on their consent;
- the PIP has processed personal information in violation of laws or administrative regulations or in breach of their agreement (*e.g.* privacy notice) with individuals; or
- other circumstances provided by laws or administrative regulations apply; and

If the retention period stipulated in law has not expired or if it is technically impossible to delete personal information concerned, the PIP should cease any unnecessary processing of personal information except for storage and adoption of necessary security protection measures.

- Request that a PIP provide an explanation of the rules governing the processing of their personal information.

The PIPL also provides any organization or individual, who may not be personal information subjects, with a right to lodge a complaint with or report to Chinese personal information protection authorities in respect of an illegal personal information processing activity. The authorities must handle the case and inform the person who lodged the report of the outcome. This type of mechanism resembles the reporting or complaint mechanisms used in the EU.

14. In what circumstances is the appointment of a data protection officer ("DPO") required?

PIPs that processes an aggregate volume of personal information that surpasses certain thresholds have to designate a DPO. Also, all CII operators will have to designate a DPO. The DPO position under the PIPL is similar in scope to the DPO position under the GDPR, which also requires entities to designate a DPO only if it meets certain conditions, such as processing special categories of personal information "on a large scale."

Pursuant to the PIPL, the DPO's name and contact details need to be reported to Chinese personal information protection authorities, and the DPO's contact details should be included in the privacy notice (although we tend to believe that a non-personally-identifiable service hotline or email address (*e.g.* privacy@ABCcompany.com) may also suffice, so long as a designated personnel is supervising and accepting inquiries made through such channel).

15. What are restrictions and requirements for marketing and the use of automated decision-making technologies and marketing?

Marketing or advertising is in general only permissible in China pursuant to the consent or on the request of recipients, and an easily opt-out channel should always be made available to recipients.

The term "**automated decision-making**" means under the PIPL as the activity of using personal information for purposes of automated analysis and evaluation of an individual's behavior, habits, interests or hobbies or an individual's economic situation, health or credit status, etc., and for decision-making, by means of computer programs.

While performing user profiling, analyzing users' preferences and sending marketing communications to users are not prohibited under the PIPL, the PIPL requires PIPs to **provide users with an option to receive marketing communications that are not specific to their personalized features or user profiles**. Where the use of automated decision-making technologies will have significant impact on the rights and interests of individuals, the individuals should have a right to request PIPs for explanation and refuse PIPs to make decisions based solely on the automated-decision-making means. PIPs will need to conduct a security impact assessment pursuant to the SIA Guidance before using personal information for automated decision-making.

16. Will GDPR-liked sanctions be applicable to breach of the PIPL?

Contravening the PIPL may result in regulatory and administrative fines, civil liability and criminal liability.

- Regulatory and administrative penalties: Like the GDPR, the PIPL establishes fines for serious breaches that are measured in proportion to the yearly turnover of the institutional offender. **For a severe violation of the law or in the absence of required data security measures, Chinese personal information protection authorities may impose a fine of the greater of: (i) RMB 50 million** (the analogous maximum under the

For a severe breach of the PIPL, the administrative fine can be up to (i) RMB 50 million or (ii) 5% of the offending entity's annual turnover in the preceding year, whichever is greater.

GDPR is EUR 20 million); **and (ii) 5% of the offending entity's annual turnover in the preceding year** (the analogous maximum under the GDPR is 4% of global annual turnover). It is unclear whether the reference to annual turnover in the PIPL refers to worldwide turnover or domestic turnover generated from the Chinese market, which is expected to be clarified in the implementation rules. Additional administrative sanctions include the **warning, confiscation of illegal gains (if any), suspension or shutdown of relevant business, or revocation of operating permit or business license**.

The leading officer directly in charge or other directly responsible persons may be subject to a fine of up to RMB 1 million, and may further be prohibited to take on director, supervisor, senior management or DPO roles in relevant company within a certain period.

- Civil liability: Under the PIPL, where the processing of personal information infringes upon the rights and interests of individuals and causes harm, and the PIP cannot prove that it was not at fault, the PIP shall bear liability for the infringement such as liability for damages. The liability for damages should be principally determined according to the loss suffered by the individual, or the gain obtained by the PIP, as a result of the infringement. **In the civil proceedings, burden of proof is shifted to the PIP in proving that it has no misconduct.**

  The PIPL also enables the **public interest class action** where a PIP contravenes the PIPL and infringes upon the rights and interests of many individuals. In such event, the People's Procuratorate, a statutory consumer organization or an organization determined by the CAC may institute an action with a People's Court.

- Criminal liability: Under the *Criminal Code of the PRC*, a penetrator who illegally sells or otherwise illegally provides personal information to third parties may be subject to a fixed-term imprisonment of not more than three years or criminal detention (or in a severe case, a fixed-term imprisonment of not less than three years but not more than seven years), and concurrently or separately, sentenced to a penalty. Where the penetrator is an entity, it would be sentenced to a penalty, while the directly responsible persons would be subject to imprisonment or criminal detention in accordance with the foregoing.

Contact Us

Zhenyu (Jay) Ruan
Senior Counsel, Shanghai
Zhenyu.Ruan@bakermckenziefenxun.com

Tingting Gao
Associate, Shanghai
Tingting.Gao@bakermckenziefenxun.com