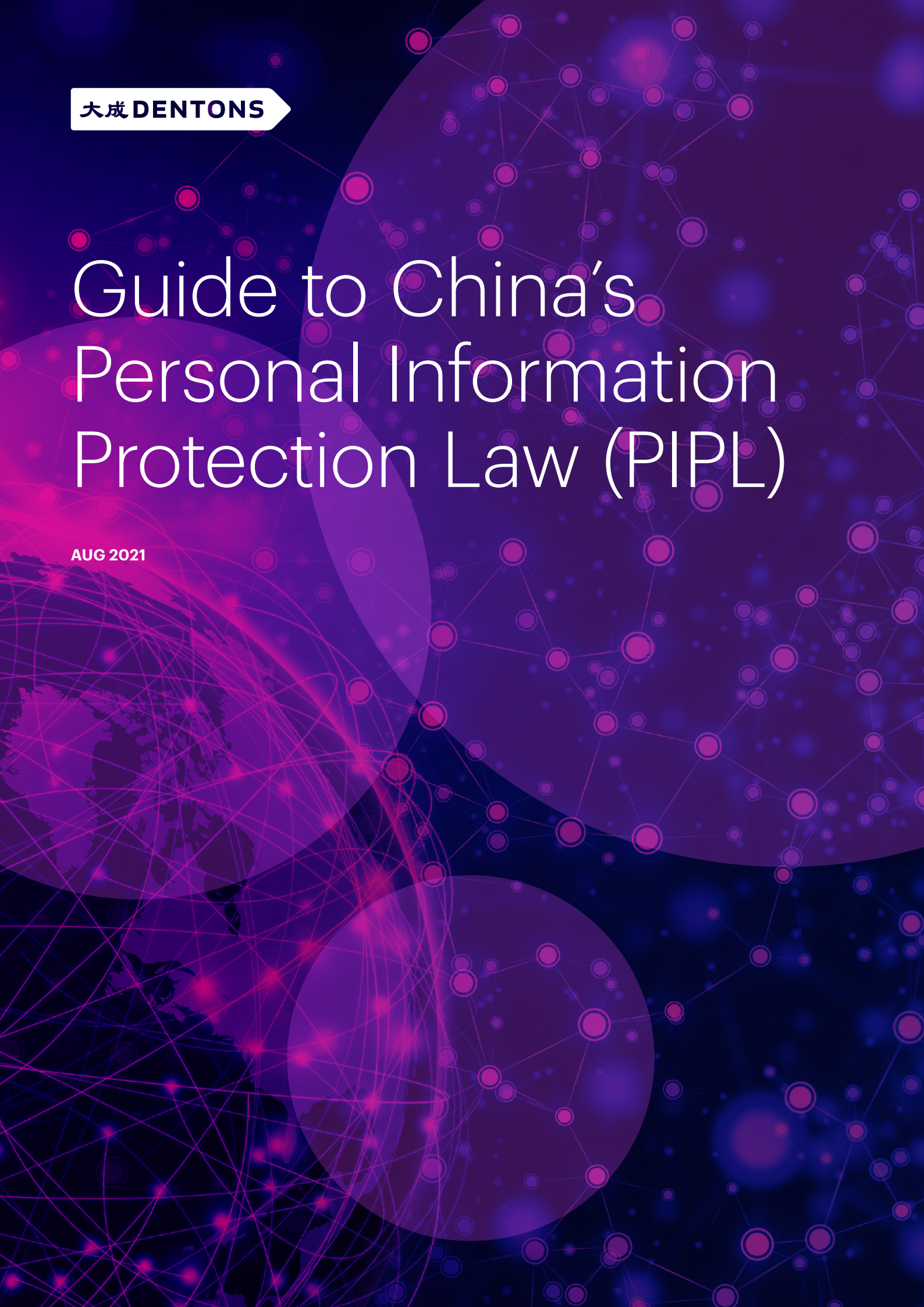
大成 DENTONS

Guide to China's Personal Information Protection Law (PIPL)

AUG 2021



Contents

Ken Dai
Partner
Shanghai, China
D +86 139 1611 3437
jianmin.dai@dentons.cn
dentons.com/en/jianmin-dai

Ken Dai has been one of the pioneering lawyers in China advising on the areas of data protection & privacy, and cybersecurity since 2012. He has rich experience in various aspects of this increasingly important field, including but not limited to reviewing and revising privacy policies, analyzing the feasibility of business modes from the perspective of data and privacy protection, issuing compliance opinions on cross-border transfer of data, employees' privacy compliance, data due diligence in M&A and joint venture transactions, and the intersection between big data and competition.

Jet Deng
Partner
Beijing, China
D +86 135 2133 7332
zhisong.deng@dentons.cn
dentons.com/en/zhisong-deng

In 2012, Mr. Deng began to engage in the cybersecurity and data protection legal practice. He has been paying close attention to China's data protection legislation for many years. Based on a deep understanding of China's legal regime of data protection & privacy and cybersecurity, he has advised numerous domestic and foreign clients on establishing compliance systems, designing business models, and coping with administrative investigations and civil litigations. He has also assisted companies in solving problems involving collection, processing, privacy protection, and cross-border transfer of client and employee information on many occasions.

Introduction

The long-expected and widely-concerned *Personal Information Protection Law of the People's Republic of China* ("PIPL") was adopted on 20 August 2021, at the 30th Session of the Standing Committee of the 13th National People's Congress.

As a basic law for personal information protection in China, the PIPL clarifies the rules for processing personal information, the obligations of personal information handlers (and processors), and the rights of personal information subjects. Notably, the PIPL provides serious punishment for violations of this law, which includes a fine of up to CNY 50 million (about USD 7,690,000) or 5% of annual turnover of the previous year.

The PIPL will come into effect as of 1 November 2021. During the grace period, organizations operating in China and those established outside China but having to be subject to the extraterritorial effect of the PIPL, are suggested to carry out data compliance work in accordance with the PIPL to get prepared for the upcoming law.

Purpose of this Guide

This Guide aims to highlight the main principles and provisions under the PIPL. It is intended to be used by organizations as an aid to find gaps in compliance and take possible steps required in practice.

Each section of this Guide describes an important rule or requirement under the PIPL. We also provide "Actions" suggested to be considered and/or adopted for ensuring compliance.

Please note that the relevant supporting rules and regulations of the PIPL are expected to be promulgated and implemented accordingly, which is advisable to be paid close attention to. Also, other relevant laws and regulations, as well as department rules shall be taken into consideration when assessing compliance.

1. Scope and Territorial Reach

1. What Is "Personal Information"?

The PIPL borrows language from the EU General Data Protection Regulation ("**GDPR**") to define personal information as "all information *related to* identified or identifiable natural persons" (Article 4). This defining approach goes beyond China's *Cybersecurity Law* and the *Civil Code* which both consider personal information as information that "can *identify* a natural person directly or in combination with other information". Under the PIPL, information that may not identify a natural person but may be related to an identified person is still treated as personal information.

The only exception is anonymized information, as stipulated by Article 4 of the PIPL. Anonymization refers to "the process by which personal information cannot be used to identify specific natural persons and the personal information cannot be restored after processing" (Article 73).

2. What Is a "Personal Information Handler"?

Compared with the GDPR and data privacy laws of some other jurisdictions, the term of "personal information handler" in the PIPL seems unique. In fact, despite the adoption of a different word, the role of such personal information handler can be understood as the personal information controller as used in the GDPR. Article 73 of the PIPL defines such a "handler" as organizations and individuals that independently determine the processing purpose and method in personal information processing.

Although it may seem not compatible with the common discourse of data privacy, as a matter of fact, the PIPL is consistent with the *Civil Code* that came into effect in early 2021, which does not adopt the term of controller either but only the concept of "handler". To avoid confusion, readers of this Guide please bear in mind that under the PIPL, a handler means a controller.

3. What Is the Territorial Scope of the PIPL?

The most notable provision of the PIPL is probably Article 3 on the territorial scope, which extends the application of PIPL beyond processing of personal information in China to processing outside China subject to specific conditions.

a. Processing personal information within China

Similar to the "establishment" threshold under the GDPR, the PIPL applies to "processing activities of personal information of natural persons conducted by organizations and individuals *within* the territory of China." In other words, regardless of whether the processing is conducted by Chinese companies or local affiliates of multinational corporations, it is subject to the PIPL regulation as long as the organization is based in China. We understand that this can cover data processing by both handlers and processors in China.

b. Extraterritorial effect

The PIPL also applies to the processing of personal information outside China where it is for:

- the purpose of providing products and services to natural persons in China; or
- analyzing/assessing the behavior of natural persons in China; or
- such other circumstances as provided by laws and administrative regulations (unspecified in the PIPL).

The above provisions are quite similar to the "targeting" and "monitoring" criteria established by the extraterritorial application of the GDPR. However, unlike the GDPR, the PIPL does not provide further explanation as to how to evaluate the abovementioned "purpose" of providing products/services to individuals in China or what assessing the behavior of individuals means exactly. A clear answer to these questions can be vital to the enforcement of territorial scope of the PIPL.

In absence of further clarification, opinions from other Chinese rules might be referred to in practice, such as a draft national standard on data export, which considers scenarios including the use of Chinese language, acceptance of Chinese yuan for payment, and offering delivery to China as "providing products or service to China"[1]. This regulatory perspective, if adopted, will echo the GDPR to some degree.

1 See the Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comments) released by the National Information Security Standardization Technical Committee (TC260) on August 25, 2017.

Actions:

- Consider what data or information your organization is processing.
- Consider whether your organization is processing personal information within China, such as having a Chinese subsidiary, operating data centers in China, etc., and further, which subsidiaries are caught by this test.
- Consider whether non-Chinese entities (e.g. your US or EU headquarter) are conducting activities (e.g. offering products/ services or analysing behaviors) which could trigger the application of the PIPL.
- Consider segregating your data to distinguish personal information sourced from China and outside China – so we can limit the application of the PIPL as far as possible.
- Where the PIPL applies to your organization (or part thereof), comply with the obligations as set out in this Guide.

2. Key Principles

Chapter I of the PIPL includes the provisions on data processing principles, most of which resemble Article 5 of the GDPR. These principles first take shape in the *Personal Information Security Specification* (GB/T 35273-2017), a national standard that is widely referenced in practice, and its revised version in 2020 (GB/T 35273-2020) ("**PISS**").

The PIPL does not reserve the principle of consent, as under the PIPL user consent will no longer be the only lawful basis of processing personal information. In addition, the PISS had a principle of data subjects' involvement, which means to provide data subjects with channels to access, correct and erase their information, and to withdraw consents, cancel accounts, file complaints, etc. While the PIPL has a specific chapter on data subjects' rights, it is not provided as a general principle.

As general principles, these provisions set out the baseline that personal information handlers should stick to throughout the processing of personal information and should always be consulted whenever there is no directly applicable rule of a specific processing activity. Each of the key principles are stipulated below, with a summary of the key actions to help comply with each one of them.

1. Lawfulness, Necessity and Good Faith

Article 5 of the PIPL provides that the processing of personal information shall adhere to lawful and proper manners, follow the principle of necessity and good faith, and shall not process personal information through misleading, fraudulent, or coercive manners.

The principle of necessity means that the processing of personal information should be limited to what is necessary. Under the GDPR, it is part of the principle of data minimization. However, the PIPL makes a distinction between the two principles – the principle of necessity is generally applicable to all processing activities, while the principle of data minimization applies specifically to the collection of personal data (please refer to the next principle).

Good faith is not in the GDPR, though it does include a principle of fairness, which is quite close. In China, the good faith principle is a fundamental legal principle, particularly in contract law. The PIPL makes it explicit that this principle equally applies in personal information processing activities.

Actions:

- Lawfulness: Consider the lawful basis of processing personal information under Article 13 since at least one of them needs to be met. For those who are entrusted by a handler to process personal information, it is suggested to include a commitment on the lawfulness of personal information to be provided by the handler in their agreement.
- Note: For the processing of sensitive personal information, Article 28 to 32 also need to be considered.
- Necessity: Consider and clarify what kind of personal information is needed for what function of your product or service. Consider pseudonymisation.
- Good faith: Apply the good faith principle in the drafting, interpretation and fulfilling the obligations of your privacy policy, terms of use, and other legally binding documents.

2. Purpose Limitation and Data Minimization

Article 6 of the PIPL provides that the processing of personal information shall have specified and legitimate purposes, and shall be directly related to the purpose of processing and in a manner that has the least impact on personal rights and interests. The collection of personal information shall be limited to the minimum scope for the purpose of processing and shall not be excessive.

3. Transparency

Actions:

- Purpose limitation: Determine the purpose at the time of collection. When processing is not based on consent, take the following into account to assess whether the further purpose is compatible: link between purposes, context of collection, nature of personal information and consequences of further processing.
- Data minimization: Ensure you collect the minimum amount of data required.

Article 7 of the PIPL provides that the processing of personal information shall follow the principle of openness and transparency. The rules of processing personal information shall be disclosed, and the purposes, manners and scope of processing shall be clearly expressed.

Actions:

- Tell individuals how their personal information would be processed, in a way that is concise, easily accessible, easy to understand and in clear and plain language.
- Display a privacy notice when an individual opens your website or launches your app for the first time.
- Test how many clicks are required for an individual to access your privacy notice and consider whether it is reasonable.
- Consider the font and size of your privacy notice and whether it is reasonably clear for an individual to read through it.

4. Accuracy

Article 8 of the PIPL provides that, when processing personal information, the quality of personal information shall be guaranteed, and it shall be avoided that the inaccuracy and incompleteness of personal information adversely affect personal rights and interests.

Actions:

- Ensure that all data is accurate, complete and kept up to date.

5. Accountability and Security

Article 9 of the PIPL provides that personal information handlers shall be responsible for their personal information processing activities and take necessary measures to ensure the security of the personal information processed.

Actions:

- Consider what measures, including technical and organisational, are taken to secure the personal information processed.
- Consider whether these measures are adequate and effective, particularly in proportion to the amount of personal information processed, the methods and frequency of processing activities, and whether sensitive personal information is involved.
- Consider whether you have any records to demonstrate compliance, including policies, procedures, training and system logs.

3. Processing Conditions

Article 5 of the PIPL requires the personal information to be processed "lawfully". That means, the processing of personal information shall satisfy the legally provided processing conditions.

Prior to the PIPL, China adopts a consent principle in determining the lawfulness of processing personal information, which means that, unless otherwise provided by law and administrative regulation, processing of personal information should be subject to the data subject's informed consent.

In view of the limitation of the consent principle as well as the increasingly complex processing scenarios, the PIPL takes an approach similar to the GDPR, which provides multiple lawful basis for processing personal information in addition to consent. We have listed the conditions for processing all personal information and those special ones for processing sensitive personal information below.

1. Conditions for Processing All Personal Information

Article 13 of the PIPL provides seven circumstances under which may a personal information handler process personal information.

a. The data subject's consent is obtained

Consent is the most used lawful basis for processing personal information. According to Article 14 of the PIPL, the consent shall be a clear and voluntary declaration of intent under the premise of full knowledge of the individual.

Notably, the PIPL requires a "separate consent" (rather than a package consent covering all the processing purposes) to be obtained under each of the following situations:

- providing personal information to a third party,
- publicizing personal information processed,
- processing sensitive personal information,
- using personal information which is collected for public security for any other purpose, and
- transferring personal information outside the territory of China.

Besides, the PIPL stipulates that, individuals have the right to withdraw consent to the processing of personal information based on their consent, and the personal information handler shall provide them with a convenient way to withdraw consent.

b. Processing is necessary for the conclusion or performance of a contract with the data subject, or for human resources management according to lawfully formulated labour rules and lawfully concluded contracts

Applying the condition in the first half, the handler and the data subject should have or will have a contractual relationship. What's worth mentioning is that if the processing is beyond the necessary scope for the conclusion or performance of a contract, such condition shall not be relied on as a lawful basis.

The final version of the PIPL, for the first time, provides that being "necessary for human resources management" could be a lawful basis for processing personal information. Such provision is undoubtedly beneficial to employers, as consent will be no longer needed for human resources management purposes. However, in consideration of the principle of "purpose limitation and data minimization", the processing of employees' personal information shall also be limited to a necessary scope.

c. Processing is necessary for the performance of statutory duties or for compliance with legal obligations

First, such statutory duties and legal obligations shall be provided under the Chinese law, therefore disclosure requests from regulators outside China are not covered. Meanwhile, those duties and obligations shall be explicitly stipulated by law, blanket and informal ones could not be relied on as a lawful basis.

d. Processing is necessary for coping with public health emergencies or for the protection of the life, health, and property safety of a nature person

The legislative background of this paragraph is somewhat related to the COVID-19 outbreak. Similar to the above, it is required that the processing shall be "necessary" for the provided purposes, that means, processing of personal information beyond the necessary scope could not be justified based on this condition.

e. Processing personal information that has been publicly disclosed by the data subjects themselves or other legally disclosed personal information within a reasonable scope

Meanwhile, Article 27 of the PIPL provides that, where the individual clearly refuses, the personal information handler shall not process his/her personal information even such information has been legally disclosed. In addition, consent of the data subject shall be obtained in accordance with the law if the processing of personal information already disclosed may have a significant impact on the individual's rights and interests.

f. Processing personal information within a reasonable scope is to carry out such activities as news reporting and supervision by public opinions for the public interests

It is worth noting that the processing of personal information based on this condition, even if it is for the public interests, should be limited to a necessary scope. For example, to report the whereabouts of an infected person for the prevention and control of infectious diseases may be reasonable, but if other personal information of the person is disclosed at the same time such as the telephone number, it may be considered unnecessary and unreasonable.

g. Other circumstances provided by laws and administrative regulations

Those "laws and administrative regulations" shall be understood in a narrow way, which only include the laws enacted by China's National People's Congress and its Standing Committee and the administrative regulations issued by the State Council. That means, the circumstances in rules and regulations promulgated by government departments and local governments could not be regarded as lawful conditions for processing personal information.

Notably, unlike the GDPR, the PIPL does not include legitimate interest as a lawful basis for processing of personal information. Thus, the personal information handler cannot claim that "the processing is necessary for the purpose of the legitimate interests pursued by the handler or a third party".

2. Special Conditions for Processing Sensitive Personal Information

According to the PIPL, a personal information handler may not process sensitive personal information unless it has a specific purpose and sufficient necessity, and adopts strict protection measures. As the disclosure or illegal use of sensitive personal information may lead to discrimination or serious harm to personal or property safety, the PIPL provides special conditions for processing sensitive personal information.

On one hand, as above-mentioned, a "separate consent" shall be obtained before processing sensitive personal information, and if the law or administrative regulations require written consent to be obtained for the processing of sensitive personal information (which is not specified in the PIPL), the provisions shall be followed.

On the other hand, in addition to the matter to be notified to the individual when processing his/her personal information, the handler shall also inform the individual of 1) the necessity of processing sensitive personal information and 2) the impacts on the individual's rights and interests, unless otherwise provided by the PIPL.

Actions:

- Identify what processing conditions are being relied on to process personal information and sensitive personal information.
- When personal information is processed based on the data subjects' consent, ensure that:
    - the consent is a clear and voluntary declaration of intent under the premise of full knowledge of the individual;
    - the form of consent (e.g. separate consent, written consent) complies with the relevant requirements;
    - generally, the consent shall not be obtained based on pre-ticked boxes or an assumption of "silence is consent";
    - the consent of the minor's guardian is obtained before processing the minor's personal information;
    - data subjects are provided with an easy way to withdraw consent;
    - when the purpose or method of processing personal information or the type of personal information to be processed changes, the data subjects' consent shall be obtained again.
- When personal information is processed relying on other conditions, ensure that the processing is necessary to achieve the specific purpose and limited to a reasonable scope.
- No matter which condition the processing relies on, inform the data subjects of the matters required by the PIPL in an eye-catching manner and with clear and understandable language.

4. Rights of Data Subjects and Corresponding Obligations

1. Right of Knowledge, Decision, Restriction, Objection and Rescission

No matter which lawful basis the processing is based on, personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language and timely update data subjects of any changes (Article 17):

- the name or personal name and contact information of the personal information handler;
- the purpose and method of processing personal information, and the type and retention period of the processed personal information;
- the method and procedure for the individual to exercise the rights provided herein; and
- other matters to be notified in accordance with the provisions of laws and administrative regulations.

Unless otherwise provided for by laws and administrative regulations, personal information handler shall also guarantee the right of data subject to make decisions, to restrict or object to the processing of his/her personal information (Article 44).

Specifically, for those processing based on consent, the right to rescind consent is also guaranteed by the PIPL, which requires personal information handlers to provide a convenient way to withdraw consent without affecting the effectiveness of personal information processing activities undertaken on the basis of consent before consent was rescinded.

2. Right to Access, Copy and Portability

Where a data subject requests to access or copy his/her personal information, personal information handler shall provide the information in a timely manner (Article 45). Such right echoes the "right to access" under the GDPR, although the GDPR premises such right on the rights and freedom of others not being adversely affected, whereas the PIPL allows for exception only for two circumstances: (i) where laws or administrative regulations provide that secrecy shall be preserved or notification is not necessary, or (ii) where notification will impede State organs' fulfillment of their statutory duties and responsibilities. Also contrary to the GDPR, no specifications on the form and cost of such copy have been stipulated by the PIPL.

A noteworthy highlight of PIPL is the right to data portability to a designated personal information handler if conditions that are determined by the State cybersecurity and information department are met (Article 45). Instead of requiring provision of a "structured, commonly used and machine-readable format" as stipulated by the GDPR, the PIPL only requires personal information handlers to provide a channel to transfer.

3. Right to Rectification

Under the PIPL, a data subject is also entitled to request for correction or supplement when his/her personal information is found inaccurate or incomplete. Upon such request, relevant verification, corrections or supplements shall be made in a timely manner (Article 46).

4. Right to Deletion

Personal information handler shall proactively delete personal information of relevant data subjects under the following circumstances (Article 47):

- where the purpose of processing has been achieved or is no longer necessary to achieve the purpose of processing;
- where the personal information handler stops providing products or services, or the retention period has expired;
- where the individual withdraws his/her consent;
- where the personal information handler processes personal information in violation of laws, administrative regulations or the agreement; or
- any other circumstance as prescribed by laws and administrative regulations.

If the personal information handler fails to delete under the abovementioned circumstances, the data subject has the right to request deletion.

Noticeably, if the retention period stipulated by laws or administrative regulations has not expired, or if the deletion of personal information is technically difficult to achieve, the personal information handler shall

cease processing other than storing and taking the necessary security protection measures.

5. Automated Decision-Making

Where personal information is used to make automated decision, personal information handler shall guarantee the transparency of decision making and the fairness and justice of processing results (Article 24).

Where a data subject believes that automated decision-making has a significant impact on his/her rights and interests, the data subject has the right to require the personal information handler to give an explanation, and to refuse that personal information handlers make decisions solely through automated decision-making methods.

Where business marketing and push notifications are carried out through automated decision-making, personal information handler shall provide either option not based on his/her personal characteristics or option for refusal. In this regard, the PIPL is similar to the GDPR.

Actions:

- Evaluate and update current mechanisms to guarantee transparency of the processing of data subjects' personal information.
- Train employees responsible for data subject requests and raise awareness of personal information protection.
- Upgrade IT tools or resources to act promptly to data subjects exercising rights vigorously.
- Review and identify personal information that need proactive deletion and continuously monitor on data retention practices.
- Conduct periodic audit on the fairness and reasonableness of automated decision-making process and provide opt-out options.

5. Data Governance and Security

The PIPL expressly legislates for what has been considered mandatory obligations in data governance and security. Among these obligations are:

1. Compliance and Security Measures

Handlers are required to take necessary measures in accordance with the purpose of processing, processing method, type of personal information, impact on individuals' rights, possible security risks, etc, to ensure that the personal information processing activities comply with the laws and regulations. Handlers should also prevent personal information from unauthorized access, being leaked, tampered with, or lost. Such measures include:

- formulating internal management systems and operating procedures;
- implementing the categorized management of personal information;
- adopting technical security measures such as encryption, de-identification, etc.;
- reasonably determining the operation authorizations of the persons processing personal information, and regularly providing security education and training to them; and
- establishing and implementing emergency plans of personal information security incidents.

2. Appointment of the "DPO"

Handlers who process personal information in a volume as specified by the state cyberspace and informatization department shall designate a "personal information protection officer" responsible for supervising data processing activities and protective measures adopted.

Under the PIPL, the contact information of the personal information protection officer needs to be disclosed to the public. The name and contact information of this officer shall also be submitted to the authority.

3. Appointment of Representative

Handlers outside China which are subject to the exterritorial effects of PIPL need to establish a dedicated office or appoint a designated representative in China, to be responsible for handling matters related to the protection of personal information. However, it remains unclear what the specific role of such an office or representative is and whether it can be like a "contact point" of the handler, like the role of a representative under the GDPR.

Besides, the name of the relevant entity (office) and the name and contact information of the representative should be submitted to the authority as well.

4. Audit

For the first time, the PIPL has included compliance audit of personal information as an obligation into the Chinese law. Handlers are required to conduct compliance audits on whether their personal information processing activities are compliant on a regular basis.

Audit can also be part of an enforcement action. Where the authority discover relatively high risk exists resulting from personal information processing activities, or observe the occurrence of personal information security incidents, it may request the handler to engage professional institutions to conduct compliance audit.

5. Personal Information Protection Impact Assessment

The PIPL has established a DPIA-alike mechanism. It imposes the obligation of personal information protection impact assessments on handlers before processing data in certain circumstances so as to facilitate handlers to fully identify the risk of data processing, the impact on individuals and whether sufficient security measures have been taken.

a. When is a personal information protection impact assessment required?

The handlers shall assess the risks of the following processing activities in advance and make records of data processing:

- processing sensitive personal information;
- using personal information for automated decision-making;
- entrusting others to process personal information, providing other handlers with personal information and publicly disclosing personal information;
- transferring personal information overseas; and
- conducting other personal information processing activities that have a significant impact on individuals' rights.

b. What issues need to be assessed?

Under the PIPL, a personal information protection impact assessment shall cover three main aspects:

- whether the purpose, manner and other aspects of processing personal information are legitimate, proper and necessary;
- the impact on individuals' right and the risk level; and
- whether the security measures adopted are legitimate, effective and appropriate to the risk level.

The PIPL also requires that the assessment reports and relevant records of processing status shall be retained for at least three years.

6. Data Breach Response

The PIPL provides obligations of notification to the authority and individuals and taking remedial measures immediately after a data breach.

For further details, please refer to the ***Section 7 Data Breach Notification*** of this Guide.

7. Gatekeeper Obligations of Internet Giants

The PIPL introduces a set of enhanced obligations for handlers that operate "important" internet platform services to "massive" number of users (without providing a threshold number) and have complex business types. Such obligations include:

- establishing and improving the personal information protection compliance program in accordance with relevant regulations and establishing a steering committee independent of the handler to oversee its protection of personal information;
- formulating platform rules and clarifying the rules of processing personal information and the obligations to protect personal information for product or service providers on the platform in accordance with the principles of openness, fairness and impartiality;
- suspending services to product/service providers operating within the handler's platform if they are in serious violation of data protection laws; and
- issuing regular social responsibility reports concerning the processing of personal information.

These requirements trace recent EU developments for platform companies in the Digital Market Act and Digital Services Act (DMA/DSA).

8. Obligations of Processors

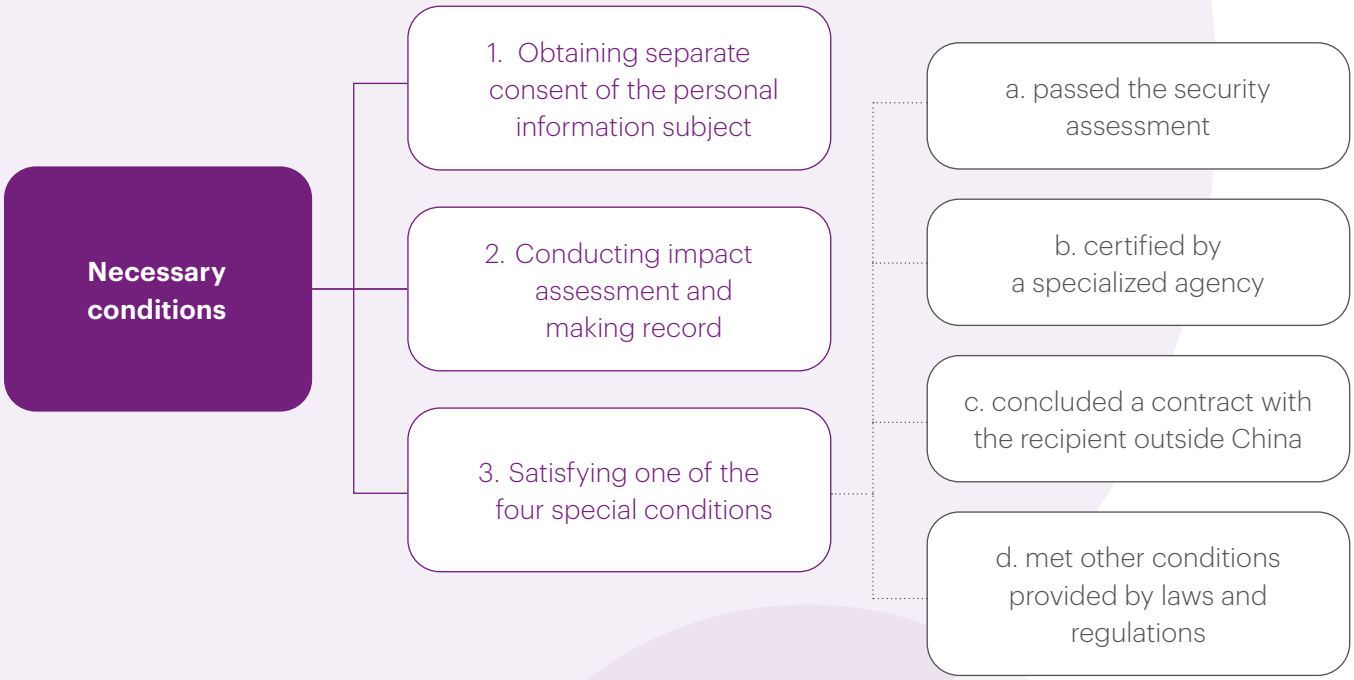
Under the PIPL, parties that are entrusted to process personal information are required to, in accordance with relevant laws and regulations, adopt necessary measures to ensure the security of personal information and assist personal information handlers in fulfilling their obligations under this law.

Actions:

- Review the policies, procedures, and technical measures currently in place to ensure the protection of personal information and assess whether these measures are adequate.
- Provide training and education to employees processing personal information and key roles in business development, marketing, information security etc.
- Consider whether a personal information protection officer (or a DPO) is required and who would most appropriately take this position within your organisation. Disclose the officer's contact information and submit relevant information to the authority.
- Consider whether a local office or representative is needed if your organization is a handler outside China.
- Establish a periodic compliance auditing mechanism on personal information protection.
- Establish personal information protection impact assessment policies, procedures as well as template documents, and make impact assessment a necessary consideration for the development of new products or new businesses.
- Review any third-party agreements with processors to ensure that applicable obligations are followed.
- Evaluate whether the gatekeeper obligations of Internet giants are needed.

6. Data Transfer Outside China

According to the PIPL, in general, transferring personal information outside the territory of China shall meet three necessary conditions, namely (1) obtaining the personal information subject's separate informed consent; (2) conducting personal information protection impact assessment and making record; and (3) satisfying one of the four special conditions, as shown in the chart below.



1. Separate Informed Consent

According to the PIPL, where a personal information handler provides personal information of an individual to a party outside the territory of China, it shall obtain the individual's "separate consent" after the individual has been informed of such matters as the name of the overseas recipient, contact information, purpose and method of processing, types of personal information and the way for the individual to exercise the rights against the overseas recipient. Obtaining separate consent would not be compulsory if the legal basis for the processing of personal information is not "consent".

Such "separate consent" is expected to be further clarified in the future, while it is supposed that separate consent requires consent to be obtained separately for a specific matter, and a package consent covering all the processing purposes will not be allowed.

2. Personal Information Protection Impact Assessment

The PIPL requires personal information handlers to assess in advance the impacts of certain processing activities that include transferring personal information overseas, and to keep a record of the processing for at least three years.

Specifically, the impact assessment shall include (1) the legitimacy, justifiability and necessity of the purpose and method of transferring personal information outside China; (2) the impact on individuals' rights and interests and the degree of security risks; and (3) whether the security protection measures taken are legitimate, effective, and appropriate to the degree of risks.

3. Special Conditions

Apart from separate consent and impact assessment, the PIPL also provides that when transferring personal information outside the territory of China, at least one of the following conditions shall be met.

a. Pass the security assessment organized by the state cyberspace and informatization department

The PIPL expands the applicable scope of localization and security assessment requirement under Article 37 of the *Cybersecurity Law,* by providing that critical information infrastructure operators ("**CIIOs**") and personal information handlers whose processing of personal information reaches a certain amount should store the personal information collected and generated in China within the territory of China, where such personal information needs to be provided abroad, security assessment shall be conducted in advance.

b. Get the certification of personal information protection

The PIPL itself does not explain what it is and how to get such a certification, but it is supposed that such certification may be somewhat similar to the certification under the GDPR.

c. Enter into a contract with the overseas recipient in accordance with the standard contract formulated by the state cyberspace and informatization department

It is expected that such standard contract specifying the rights and obligations of both parties shall be similar to the standard contractual clause (SCC) under the GDPR.

d. Meet other conditions prescribed by laws, administrative regulations, or the state cyberspace and informatization department

Such catch-all clause leaves space for other specific conditions on cross-border transfer of personal information, for example, the *Administrative Regulations on Human Genetic Resources* requires the approval of the Ministry of Science and Technology to be got in advance when transferring human genetic resources abroad.

Also, the PIPL requires the personal information handler to take necessary measures to ensure that the overseas recipient's processing of personal information meets the standards for personal information protection prescribed under the PIPL.

4. Request for Personal Information by Overseas Authorities

The PIPL specifically stipulates that without the approval of the Chinese competent authority, personal information stored in China shall not be provided to judicial or law enforcement agencies outside China. Such provision is in line with that under the newly released the *Data Security Law* of China. In this regard, when participating in judicial procedures or confronting administrative investigations outside of China, attentions shall be paid to relevant requirements under the laws and regulations such as the *International Criminal Judicial Assistance Law* of China.

Actions:

- Consider whether your organization has business need of transferring personal information outside China (including remote access to data stored in China from abroad).
- Ensure that the data subjects' separate informed consent is obtained before transferring their personal information outside China if the legal basis for personal information processing is consent.
- Establish a personal information protection impact assessment mechanism for cross-border data transfer and keep the assessment report and the record of transfer for at least three years.
- Consider which special condition is the most suitable for your organization. For example, generally, CIIOs and entities with large number of personal information shall pass the security assessment; and other entities could transfer based on certification or a standard contract.
- Review and check if there are sectoral regulations that provide restrictions on cross-border data transfer, for example, special approval / license shall be obtained before transfer.
- Consider getting the approval of the relevant Chinese authority on provision of personal information to overseas authorities, when participating in judicial procedures or confronting administrative investigations outside of China.

7. Data Breach Notification

Similar to the GDPR, Article 56 of the PIPL provides a duty to report data breaches to the relevant supervisory authority and, in certain cases, to the individuals affected. Linguistically, Article 56 also delineates what data breach means as it provides that the duty attaches where personal information has or may have been leaked, tampered with or lost. However, the duty is imposed only on personal information handlers. Nonetheless, handlers could require processors of a timely notification upon a data breach in their data processing agreements.

Pursuant to Article 56, a personal information handler shall immediately notify competent authorities and individuals. The notification must include:

- the categories of personal information, the reason and the damages that may be caused of what has or may have been leaked, tampered with or lost;
- the remedial measures that are taken by the personal information handler and the measures available to an individual to mitigate the damages; and
- the contact information of the handler.

Notifying the authority is a mandatory obligation under the PIPL, while notifying individuals is not. Where a personal information handler is able to take measures to effectively avoid harm caused by the breach, it is not obliged to notify the affected individuals. But if the authority considers that the data breach may cause harm to individuals, it can require the personal information handler to notify the affected individuals.

Other than the general requirement of "immediate notification", the PIPL does not provide a specific time limit for notifying the authority or affected individuals.

Actions:

- Consider whether your organisation is a handler or a processor. (If a handler) review your agreements with processors to ensure any data breaches are agreed to be reported to you without undue delay. (If a processor) review your agreements with processors to understand your notification obligations.
- Develop and implement a Data Breach log.
- Assess the level of risk associated with data breach within your organization and the exposure to a "high risk" breach (i.e. whether you process sensitive personal data, medical data, children's data, etc. and in what volume).
- Ensure protocols are in place to ensure staff are trained regularly (e.g. every year) to recognize and act upon any data breaches.
- Consider the manners of notifying individuals, whether individual notification is possible and, if not, whether a public notification would be effective.
- Check sectoral rules for any time limit of data breach notification that may apply.

8. Managing External Flows of Data

1. Impact Assessment Prior to Engaging Third Parties

Prior to sharing personal information with a third party or entrusting a processor (such as an IT vendor), organizations should carry out impact assessment. If personal information is transferred to a foreign recipient outside China, as above-mentioned, cross-border transfer of personal information should also be a focus of such impact assessment.

Specifically, the impact assessment shall cover three main aspects:

- whether the purpose, method and other aspects of sharing personal information are legitimate, proper and necessary;
- the impact on individuals' rights and interests and the degree of security risks; and
- whether the security protection measures adopted are legitimate, effective and appropriate to the risk level.

For further requirements of the impact assessment, please refer to ***Section 5 Data Governance and Security*** of this Guide.

2. Managing Data Sharing Between Handlers

Where a handler shares personal information to a third-party handler, it shall:

- inform individuals of the third party's name, contact information, purpose, method, and types of personal information for processing; and
- obtain the "separate consent" of the individual.

Under these requirements, handlers may need to modify their current privacy notices accordingly and disclose all the necessary information related to data sharing. "Just-in-time" notices can also be a useful tool for fulfilling this obligation. For separate consent, as mentioned above, in absence of further clarification, we consider that it should be at least an informed and unambiguous consent, separate from an individuals' consent to other processing activities of his/her personal information. For example, a mobile app may ask for the user's consent to sharing personal information through a specific pop-up notification and a consent button.

In using data shared by others, the third-party handler (recipient) is obliged to stay within the scope of processing purpose and method that are informed to individuals. If the third party changes the original processing purpose or method, it shall inform the individuals and re-obtain their consent.

3. Processor Contracts

The PIPL contains prescriptive requirements regarding the detail of what must be covered in a contract with the processor (i.e. an entrusted party). The key requirements include (this is not an exhaustive list):

- the purpose and period of the entrustment of processing;
- the processing method and the types of personal information;
- the protection measures; and,
- the rights and obligations of both parties.

The handler should also supervise the processing activities of the processor.

4. Processor's Obligations

As a processor, it shall process personal information in accordance with the contract with the handler, and shall not process personal information beyond the agreed purpose of processing, processing method, etc. Where the contract is not effective, void, withdrawn, or terminated, the processor is required to "return" the personal information to the handler or destroy it.

Without the approval of the handler, the processor shall not delegate others (i.e. sub- processors) to process personal information.

In addition, the processor should also perform security obligations provided for the handler in the PIPL and adopt necessary measures to ensure data security. These obligations include formulating internal management policies and operating procedures on data protection, adopting encryption and other technical measures, appointment of the personal information protection officer, etc.

For further details of these obligations, please refer to ***Section 5 Data Governance and Security*** of this Guide.

5. External Flow of Data due to Company Changes

As a result of M&As, separations, dissolution, declaration of bankruptcy, and other such reasons, personal information may be provided to a new handler as part of data assets. According to the PIPL, the handler should notify individuals of the name and contact information of the receiving party (i.e. the new handler), which should continue to perform the obligations of the previous handler. If the new handler changes the original purpose and method of processing, the consent of individuals should be obtained again.

Actions:

- Make impact assessment a required procedure before providing data to third parties.
- Based on the results of impact assessment, take appropriate security and other measures to safeguard data transfer.
- Update the privacy notices to fully disclose to individuals the relevant information concerning transferring their data to third parties.
- Obtain individuals' separate consent for data sharing.
- Review the data processing agreement with vendors and consider whether it contains clauses required by the PIPL.
- Establish a vendor management policy and supervise vendors to fulfill their personal information protection and security obligations.
- Carry out data protection due diligence for M&As and evaluate whether consent is required for data transfer.

9. Enforcement Authorities, Liabilities and Fines

With respect to the law enforcement, the PIPL clarifies the departments performing personal information protection duties, and provides the legal liabilities for violations of the law.

1. Enforcement Authorities Responsible for Personal Information Protection

China does not have an independent data protection authority like the European countries. Instead, several departments like the Cyberspace Administration of China ("**CAC**") and the Ministry of Public Security ("**MPS**"), and their local counterparts, have certain law enforcement power over personal information protection-related issues. The PIPL does not change the current polycentric supervision system, but clarifies that:

- State cyberspace and informatization department (namely the CAC) is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work;
- relevant departments of the State Council (like the MPS, the State Administration for Market Regulation, and sectoral authorities, for example, the People's Bank of China and the National Health Commission) are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities; and
- relevant departments of county-level and higher local governments perform personal information protection duties according to related regulations.

In enforcement activities, the following measures could be taken by the authorities according to the PIPL:

- interviewing relevant concerned parties, and investigating personal information processing activities;
- looking up and copying the concerned party's contracts, records, receipts as well as other relevant material related to personal information processing activities;
- conducting on-side inspections, and investigating suspected unlawful personal information processing activities; and
- inspecting the equipment and articles relevant to personal information processing activities, and when there is evidence the equipment or articles are used in illegal personal information processing activities, after reporting to the department's main responsible person in writing and receiving approval, the equipment or articles could be sealed or confiscated.

Besides, the PIPL also stipulates that the enforcement authority may have a talk with the personal information handler's legal representative or main responsible person; or require the personal information handler to entrust specialized institutions to conduct compliance audits of its personal information processing activities, if relatively large risks are found in personal information processing activities.

2. Legal Liabilities

The PIPL provides the administrative liabilities for violations of the law. In the meantime, civil liabilities, criminal liabilities and other legal consequences are also clarified and/or mentioned thereunder.

a. Administrative liabilities

Processing personal information in violation of the PIPL, or failing to adopt necessary security protection measures when processing personal information may incur administrative liabilities under the PIPL. The PIPL stipulates two-level legal liabilities based on the severity of circumstances, for both entities and individuals that violate the law and the directly responsible persons of the violators, as follows.

It is noteworthy that, as the fine ceiling is 5% turnover in severe circumstances, the PIPL provides that only enforcement authorities at provincial or higher (i.e. national) level have the power to impose the severe level penalties.

In General Circumstances	Entities / Individuals	• Order to rectify • Warning • Confiscation of illegal gains • Order to suspend or terminate service provision of the application programs unlawfully processing personal information • A fine of not more than CNY 1 million (about USD 153,700), if refusing to make corrections
	Responsible Persons	A fine ranging from CNY10,000 (about USD 1,537) to CNY100,000 (about USD 15,370)
In Severe Circumstances	Entities / Individuals	• Order to rectify • Confiscation of illegal gains • A fine of not more than CNY 50 million (about USD 7,690,000) or **5%** of the annual turnover of the prior year • Suspension of relevant business activities, cessation of business for rectification, and/or revocation of business license or permits
	Responsible Persons	• A fine ranging from CNY 100,000 (about USD 15,370) to CNY 1 million (about USD 153,700) • Prohibition from holding positions of director, supervisor, senior manager, or personal information protection officer for a certain period

b. Civil liabilities

Generally, the data subjects whose personal information-related rights and interests have been infringed can seek civil remedies in accordance with the *Civil Code* and other laws like the *Consumer Rights Protection Law*.

But notably, the PIPL establishes the standard of "presumptive fault", which means that a personal information handler shall be liable for the damage caused by processing personal information unless it can prove it is not at fault.

Meanwhile, the PIPL also mentions the public interest litigation, by providing that the people's procuratorate, statutorily designated consumer organizations, and organizations designated by the State cyberspace and informatization department may file lawsuits, if the processing activities infringe upon the rights and interests of a large number of individuals.

c. Criminal liabilities

Pursuant to the PIPL, where a violation of this law constitutes a violation of public security administration, a public security administration punishment shall be imposed; and if a crime is constituted, criminal liability shall be pursued accordingly. For example, under the *Criminal Law* of China, if the crime of "infringing on citizens' personal information" is constituted, depending on the seriousness of the circumstances, imprisonment up to seven years plus a fine may be imposed.

d. Other legal consequences

In addition to the legal liabilities above, the PIPL also provides that violations of the PIPL will be recorded in the credit file and made public. As China's credit system continues to improve, violation records in credit files can have a negative impact on corporate development and reputation.

Actions:

- Keep good communication with the relevant enforcement authorities.
- Set up data compliance system, and conduct compliance trainings for employees.
- Establish response mechanism for administrative investigations, and conduct mock exercises, if necessary.

Appendix 1: Glossary

1. Personal Information Handler

Organizations and individuals that independently determine the processing purpose, method, and other matters of personal information processing. The role of the personal information handler under the PIPL can be understood as the personal information controller as used in the GDPR.

2. Processor

Organizations and individuals that process personal information entrusted by a personal information handler.

3. Critical Information Infrastructure Operator

The network system in the sectors of public telecommunication and information services, energy, communication, water resource, finance, public service and electronic public service, of which the damage, loss of functionality or data breach would seriously damage China's national security, economy, people's livelihood and public interest.

4. Automated Decision-making

Activity concerning the use of computer programs to automatically analyze or assess individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status, etc., and engage in decision-making activities.

5. De-identification

The process by which personal information is processed in such a way that it cannot be used to identify a specific natural person without the help of additional information.

6. Anonymization

The process by which personal information is processed in such a way that it cannot be identified with a specific natural person and cannot be recovered.

7. Sensitive Personal Information

The personal information which, once leaked or illegally used, may easily cause harm to the dignity of natural persons or grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

8. Enforcement Authorities Responsible for Personal Information Protection

A general term which covers (1) the state cyberspace and informatization department (namely the CAC); (2) relevant departments of the State Council; and (3) relevant departments of county-level and higher local governments which perform personal information protection duties according to related regulations.

Appendix 2: Personal Information Protection Law of the People's Republic of China

中华人民共和国个人信息保护法	**Personal Information Protection Law of the People's Republic of China**
目 录	Table of Contents
第一章 总 则	Chapter I: General Provisions
第二章 个人信息处理规则	Chapter II: Rules of Processing of Personal Information
第一节 一般规定	Section 1: General Rules
第二节 敏感个人信息的处理规则	Section 2: Rules of Processing Sensitive Personal Information
第三节 国家机关处理个人信息的特别规定	Section 3: Special Provisions on Processing of Personal Information by State Agencies
第三章 个人信息跨境提供的规则	Chapter III: Rules of the Cross-Border Provision of Personal Information
第四章 个人在个人信息处理活动中的权利	Chapter IV: Rights of Individuals in Activities of Processing of Personal Information
第五章 个人信息处理者的义务	Chapter V: Obligations of Personal Information Handlers
第六章 履行个人信息保护职责的部门	Chapter VI: Authorities Performing Personal Information Protection Duties
第七章 法律责任	Chapter VII: Legal Liability
第八章 附 则	Chapter VIII: Supplemental Provisions
第一章 总 则	**Chapter I: General Provisions**
第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。	Article 1: This Law is formulated, on the basis of the Constitution, in order to protect personal information rights and interests, standardize personal information processing activities, and promote the reasonable use of personal information.
第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。	Article 2: The personal information of any natural person shall be protected by law, and no organization or individual may infringe upon the personal information rights and interests of any natural person.

在中华人民共和国境内处理自然人个人信息的活动，适用本法。 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法： （一）以向境内自然人提供产品或者服务为目的； （二）分析、评估境内自然人的行为； （三）法律、行政法规规定的其他情形。	Article 3: This Law shall apply to any activity of processing of personal information of a natural person that is carried out within the territory of the People's Republic of China. This Law shall also apply to any activity of processing of personal information of any natural person located within the territory of the People's Republic of China that is carried out outside the territory of the People's Republic of China under any of the following circumstances: 1. Where the purpose of the activity is to provide a product or service to that natural person located within China; 2. Where the purpose of the activity is to analyze or assess the behavior of that natural person located within China; or 3. Any other circumstance as provided by law or administrative regulations.
第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。	Article 4: Personal information refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized. Processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.
第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。	Article 5: Personal information shall be processed in accordance with the principles of legality, legitimacy, necessity and good faith, and not in any manner that is misleading, fraudulent or coercive.
第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。 收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。	Article 6: Processing of personal information shall be for a specified and reasonable purpose, and shall be conducted for a purpose directly relevant to the purpose of processing and in a way that has the least impact on personal rights and interests. Collection of personal information shall be limited to the minimum scope necessary for achieving the purpose of processing and shall not be excessive.
第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。	Article 7: Personal information shall be processed in accordance with the principles of openness and transparency, with the rules of processing of personal information disclosed, and the purpose, method and scope of processing expressly stated.
第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。	Article 8: The quality of personal information shall be ensured when the personal information is processed in order to avoid any negative impact on personal rights and interests due to any inaccuracy or incompleteness of the personal information processed.
第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。	Article 9: Personal information handlers shall be responsible for their activities of processing of personal information, and take necessary measures to ensure the security of the personal information processed.
第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。	Article 10: No organization or individual may illegally collect, use, process, or transmit other persons' personal information, or illegally sell, buy, provide, or disclose other persons' personal information, or engage in personal information processing activities harming national security or the public interest.

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。	Article 11: The State will establish a sound personal information protection regime to prevent and punish any act of infringement of personal information rights and interests, strengthen publicity and education on personal information protection, and promote the creation of a sound environment for the government, enterprises, relevant trade organizations, and the public to jointly participate in personal information protection.
第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。	Article 12: The State will actively participate in the development of international rules for personal information protection, promote international exchange and cooperation in personal information protection, and promote the mutual recognition of the rules and standards of personal information protection with other countries, regions, and international organizations.
第二章 个人信息处理规则	**Chapter II Rules of Processing of Personal Information**
第一节 一般规定	Section 1: General Rules
符合下列情形之一的，个人信息处理者方可处理个人信息： （一）取得个人的同意； （二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需； （三）为履行法定职责或者法定义务所必需； （四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需； （五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息； （六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息； （七）法律、行政法规规定的其他情形。 依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。	Article 13: A personal information handler may process personal information of an individual only under any of the following circumstances: 1. Where consent is obtained from the individual; 2. Where it is necessary for the conclusion or performance of a contract to which the individual is a contracting party, or where it is necessary for carrying out human resources management under an employment policy legally established or a collective contract legally concluded; 3. Where it is necessary for performing a statutory responsibility or statutory obligation; 4. Where it is necessary for responding to a public health emergency, or for protecting the life, health or property safety of a natural person in the case of an emergency; 5. Where the personal information is processed within a reasonable scope to carry out any news reporting, supervision by public opinions or any other activity for public interest purposes; 6. Where the personal information, which has already been disclosed by the individual or otherwise legally disclosed, is processed within a reasonable scope and in accordance with this Law; or 7. Any other circumstance as provided by law or administrative regulations. Personal consent shall be obtained for the processing of personal information as required by the other provisions of this Law, but where any of the preceding Items 2 to 7 is applicable, personal consent is not required.
基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。	Article 14: Where personal information is to be processed based on consent of an individual, such consent shall be a voluntary and explicit indication of intent given by such individual on a fully informed basis. Where specific consent or written consent shall be obtained from individuals for the processing of their personal information as provided by any law or administrative regulations, such provision shall prevail. In the event of any change of the purpose or method of processing or the type of personal information to be processed, personal consent shall be obtained again.

基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

Article 15: Individuals shall have the right to withdraw their consent to the processing of their personal information carried out based on their consent. Personal information handlers shall provide an easy way to withdraw consent.

A withdrawal of consent by individuals shall not affect the validity of any activity of processing of their personal information already carried out before the withdrawal based on their consent.

第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

Article 16: Personal information handlers shall not refuse to provide a product or service to individuals on the grounds that they do not consent to the processing of their personal information or they withdraw their consent, unless the processing of personal information is necessary for providing the product or service.

个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：
（一）个人信息处理者的名称或者姓名和联系方式；
（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；
（三）个人行使本法规定权利的方式和程序；
（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

Article 17: Personal information handlers shall, before processing personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language:

The name or personal name and contact method of the personal information handler;

The purpose of personal information processing and the processing methods, the categories of handled personal information, and the retention period;

The method and procedure for individuals to exercise the rights provided in this Law;

Other items that laws or administrative regulations provide shall be notified.

Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified about the change.

Where personal information handlers notify the matters as provided in paragraph I through the method of formulating personal information processing rules, the processing rules shall be made available to the public and convenient to access and store.

第十八条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。
紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

Article 18: A personal information handler who is to process personal information of an individual may be allowed not to inform the individual of any matter stated in the first paragraph of the preceding Article if such matter shall be kept confidential or is not required to be disclosed according to law or administrative regulations.

If, for the protection of life, health or property safety of a natural person in the case of an emergency, an individual cannot be informed in a timely manner, the individual shall be informed in a timely manner by the personal information handler after the emergency is cleared.

第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

Article 19: Except where laws or administrative regulations provide otherwise, personal information retention periods shall be the shortest period necessary to realize the purpose of the personal information processing.

第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

Article 20: Two or more personal information handlers who jointly decide on the purpose and method of the processing of personal information shall agree on their respective rights and obligations in the joint processing, but such agreement shall not affect the right of individuals to exercise their rights provided for by this Law against any of the personal information handlers.

Personal information handlers who jointly process personal information shall be liable jointly and severally under the law for any damages caused due to an infringement of personal rights and interests in their joint processing of personal information.

第二十一条 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

Article 21: A personal information handler contracting the processing of personal information to another party shall agree with the contracted processor on the purpose, period, and method of the contracted processing, the type of personal information to be processed, any protection measure to be taken, and the rights and obligations of both parties, etc., and supervise the activities of processing of personal information carried out by the personal information processor.

Personal information processor shall process personal information as agreed, and shall not process personal information beyond the agreed purpose and method of the contracted processing; if the contract of the contracted processing fails to become effective, becomes null and void, or is cancelled or terminated, the personal information processor shall return the personal information to the contracting personal information handler or delete it, and shall not retain such information.

Without the approval of the contracting personal information handler, the personal information processor shall not subcontract the contracted processing of personal information to any other person.

第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

Article 22: A personal information handler who needs to transfer personal information of any individual due to a merger, division, dissolution, declared bankruptcy or any other reason shall inform the individual of the organizational or personal name and contact information of the receiving party. The receiving party shall continue to perform obligations of the personal information handler. For any change of the original purpose or method of processing, the receiving party shall obtain consent from the individual anew in accordance with this Law.

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

Article 23: Where personal information handlers provide other personal information handlers with the personal information they process, they shall notify individuals about the name or personal name of the recipient, their contact information, the processing purpose, processing method, and personal information categories, and obtain separate consent from the individual. Recipients shall process personal information within the above mentioned scope of processing purposes, processing methods, personal information categories, etc. Where recipients change the original processing purpose or processing methods, they shall again obtain the individuals consent.

第二十四条 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。 通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。	Article 24: When personal information handlers use personal information to conduct automated decision-making, the transparency of the decision-making and the fairness and justice of the processing result shall be guaranteed, and they may not engage in unreasonable differential treatment of individuals in trading conditions such as trade price, etc. Those conducting information push delivery or commercial sales to individuals through automated decision-making methods shall simultaneously provide the option to not target an individual's characteristics, or provide the individual with a convenient method to refuse. When the use of automated decision-making produces decisions with a material influence on the rights and interests of the individual, they have the right to require personal information handlers to explain the matter, and they have the right to refuse that personal information handlers make decisions solely through automated decision-making methods.
第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。	Article 25: Personal information handlers may not disclose the personal information they process; except where they obtain separate consent.
第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。	Article 26: The installation of image collection or personal identity recognition equipment in public venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. Collected personal images and personal distinguishing identity characteristic information can only be used for the purpose of safeguarding public security; it may not be used for other purposes, except where individuals' separate consent is obtained.
第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。	Article 27: Personal information handlers may, within a reasonable scope, process personal information that has already been disclosed by the person themselves or otherwise lawfully disclosed, except where the person clearly refuses. Personal information handlers processing already disclosed personal information, where there is a major influence on individual rights and interests, shall obtain personal consent in accordance with the provisions of this Law.
第二节 敏感个人信息的处理规则	Section II: Rules of Processing Sensitive Personal Information
第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。	Article 28: Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14. Only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures, may personal information handlers process sensitive personal information.
第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。	Article 29: To process sensitive personal information, the individual's separate consent shall be obtained. Where laws or administrative regulations provide that written consent shall be obtained for processing sensitive personal information, those provisions are to be followed.

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。	Article 30: Personal information handlers processing sensitive personal information, in addition to the items set out in Article 17 paragraph I of this Law, shall also notify individuals of the necessity and effects on the individual's rights and interests of processing the sensitive personal information, except where this Law provides that it is permitted not to notify the individual.
第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。	Article 31: Where personal information handlers process the personal information of minors under the age of 14, they shall obtain the consent of the parent or other guardian of the minor. Where personal information handlers process the personal information of minors under the age of 14, they shall establish specialized personal information processing rules.
第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。	Article 32: Where laws or administrative regulations provide that relevant administrative licenses shall be obtained or other restrictions apply to the processing of sensitive personal information, those provisions are followed.
第三节 国家机关处理个人信息的特别规定	Section III: Special Provisions on Processing of Personal Information by State Agencies
第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。	Article 33: This Law applies to State organs' activities of processing personal information; where this Section contains specific provisions, the provisions of this Section apply.
第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。	Article 34: State organs processing personal information to fulfill their statutory duties and responsibilities shall conduct them according to the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfill their statutory duties and responsibilities.
第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。	Article 35: State organs processing personal information for the purpose of fulfilling statutory duties and responsibilities shall fulfill notification duties, except where circumstances as provided in Article 18, paragraph I, of this Law exist, or where notification will impede State organs' performance of their statutory duties.
第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。	Article 36: Personal information processed by State organs shall be stored within the mainland territory of the People's Republic of China. If it is necessary to provide it abroad, a security assessment shall be undertaken. Relevant authorities may be requested to support and assist with security assessment.
第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。	Article 37: The provisions of this Law regarding personal information processing by State organs apply to organizations processing personal information in order to fulfill their duties while performing functions related to managing public affairs as authorized by laws and administrative regulations.

第三章 个人信息跨境提供的规则	**Chapter III: Rules on the Cross-Border Provision of Personal Information**
第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一： （一）依照本法第四十条的规定通过国家网信部门组织的安全评估； （二）按照国家网信部门的规定经专业机构进行个人信息保护认证； （三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务； （四）法律、行政法规或者国家网信部门规定的其他条件。 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。 个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。	Article 38: Where personal information handlers need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they shall meet one of the following conditions: Passing a security assessment organized by the State cyberspace administration according to Article 40 of this Law; Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department; Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides; Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department. Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain provisions such as conditions on providing personal data outside the borders of the People's Republic of China, it is permitted to act according to those provisions. Personal information handlers shall adopt necessary measures to ensure that foreign receiving parties' personal information processing activities reach the standard of personal information protection provided in this Law.
第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。	Article 39: Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual about the foreign receiving side's name or personal name, contact method, processing purpose, processing methods, and personal information categories, as well as ways or procedures for individuals to exercise the rights provided in this Law with the foreign receiving side, and other such matters, and obtain individuals' separate consent.
第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。	Article 40: Critical information infrastructure operators and personal information handlers processing personal information reaching quantities provided by the State cyberspace administration shall store personal information collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad, they shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cyberspace administration provisions permit that security assessment not be conducted, those provisions are followed.
第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。	Article 41: Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored domestically. Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。	Article 42: Where foreign organizations or individuals engage in personal information processing acts violating personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cyberspace administration may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.
第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。	Article 43: Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt retaliatory measures against said country or region on the basis of actual circumstances.
第四章 个人在个人信息处理活动中的权利	**Chapter IV: Rights of Individuals in Activities of Processing of Personal Information**
第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。	Article 44: Individuals have the right to know and the right to decide relating to their personal information, and have the right to limit or refuse the processing of their personal information by others, unless laws or administrative regulations stipulate otherwise.
第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。 个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。 个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。	Article 45: Individuals have the right to access and copy their personal information from personal information handlers, except in circumstances provided in Article 18, paragraph I, or Article 35 of this Law. Where individuals request to access or copy their personal information, personal information handlers shall provide it in a timely manner. Where individuals request that their personal information be transferred to a personal information handler they designate, meeting conditions of the State cybersecurity and informatization department, personal information handlers shall provide a channel to transfer it.
第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。 个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。	Article 46: Where individuals discover their personal information is incorrect or incomplete, they have the right to request personal information handlers correct or complete their personal information. Where individuals request to correct or complete their personal information, personal information handlers shall verify the personal information and correct or complete it in a timely manner. Where individuals request to correct or complete their personal information, personal information handlers shall verify the personal information and correct or complete it in a timely manner.

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除： （一）处理目的已实现、无法实现或者为实现处理目的不再必要； （二）个人信息处理者停止提供产品或者服务，或者保存期限已届满； （三）个人撤回同意； （四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息； （五）法律、行政法规规定的其他情形。 法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。	Article 47: Personal information handlers shall actively delete personal information where one of the following circumstances occurs; if the personal information handler has not deleted, individuals have the right to request deletion: The processing purpose has been achieved, is impossible to achieve, or [the personal information] is no longer necessary to achieve the processing purpose; Personal information handlers cease the provision of products or services, or the retention period has expired; The consent is withdrawn by the individual; Personal information handlers process personal information in violation of laws, administrative regulations, or agreements; Other circumstances provided by laws or administrative regulations. Where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realize, personal information handlers shall cease personal information processing except for storage and taking necessary security protective measures.
第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。	Article 48: Individuals have the right to request personal information handlers explain personal information processing rules.
第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。	Article 49: When a natural person is deceased, their next of kin may, for the sake of their own lawful, legitimate interests, exercise the rights provided in this Chapter to access, copy, correct, delete, etc., the personal information of the deceased, except where the deceased has arranged otherwise before their death.
第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。 个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。	Article 50: Personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason. Where personal information handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit with a People's Court according to the law.

第五章 个人信息处理者的义务	**Chapter V: Obligations of Personal Information Handlers**
第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； （五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。	Article 51: Personal information handlers shall, on the basis of the personal information processing purpose, processing methods, personal information categories, as well as the influence on individuals' rights and interests, possibly existing security risks, etc., adopt the following measures to ensure personal information processing conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as personal information leaks, distortion, or loss: 1. Formulating internal management structures and operating rules; 2. Implementing categorized management of personal information; 3. Adopting corresponding technical security measures such as encryption, de-identification, etc.; 4. Reasonably determining operational limits for personal information processing, and regularly conducting security education and training for employees; 5. Formulating and organizing the implementation of personal information security incident response plans; 6. Other measures provided in laws or administrative regulations.
第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。 个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。	Article 52: Personal information handlers who process personal information reaching quantities provided by the State cyberspace administration shall appoint personal information protection officers, responsible for conducting supervision of personal information processing activities as well as adopted protection measures, etc. Personal information handlers shall disclose the methods of contacting personal information protection officers, and report the names of the officers and contact methods to the authority performing personal information protection duties.
第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。	Article 53: Personal information handlers outside the borders of the People's Republic of China, as provided in Article 3, paragraph II, of this Law, shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China to be responsible for matters related to the personal information they process, and are to report the name of the relevant entity or the name and contact method, etc., of the representative to the authority performing personal information protection duties.
第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。	Article 54: Personal information handlers shall regularly engage in audits of their personal information processing and compliance with laws and administrative regulations.
第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录： 处理敏感个人信息；（二）利用个人信息进行自动化决策； （三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；（四）向境外提供个人信息；（五）其他对个人权益有重大影响的个人信息处理活动。	Article 55: When one of the following circumstances is present, personal information handlers shall conduct a personal information protection impact assessment in advance, and record the processing situation: 1. Processing sensitive personal information; 2. Using personal information to conduct automated decision-making; 3. Entrusting personal information processing, providing personal information to other personal information handlers, or disclosing personal information; 4. Providing personal information abroad; 5.Other personal information processing activities with a major influence on individuals.

第五十六条 个人信息保护影响评估应当包括下列内容:

（一）个人信息的处理目的、处理方式等是否合法、正当、必要;

（二）对个人权益的影响及安全风险;

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

Article 56: The content of the personal information protection impact assessment shall include:

Whether or not the personal information processing purpose, processing method, etc., are lawful, legitimate, and necessary;

The influence on individuals' rights and interests, and the security risks;

Whether protective measures undertaken are legal, effective, and suitable to the degree of risk.

Personal information protection impact assessment reports and processing status records shall be preserved for at least three years.

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项:

发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害;

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施;

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人;履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

Article 57: Where a personal information leak, distortion, or loss occurs or might have occurred, personal information handlers shall immediately adopt remedial measures, and notify the authority performing personal information protection duties and the individuals. The notification shall include the following items:

The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred;

The remedial measures taken by the personal information handler and measures individuals can adopt to mitigate harm;

Contact method of the personal information handler.

Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, distortion, or loss, personal information handlers are permitted to not notify individuals; however, where authority performing personal information protection duties believe harm may have been created, they may require personal information handlers to notify individuals.

第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务:

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督;

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务;

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务;

（四）定期发布个人信息保护社会责任报告，接受社会监督。

Article 58: Personal information handlers providing important Internet platform services, who have a large number of users, and whose business models are complex shall fulfill the following obligations:

1. Establish and complete personal information protection compliance structures and systems according to State regulations, and establish an independent body composed mainly of outside members to supervise personal information protection circumstances;

2. Abide by the principles of openness, fairness, and justice; formulate platform rules; and clarify the standards for intra-platform product or service providers' processing of personal information and their personal information protection duties;

3. Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in processing personal information;

4. Regularly release personal information protection social responsibility reports, and accept society's supervision.

第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

Article 59: Entrusted persons accepting entrusted processing of personal information shall, according to the provisions of this Law and relevant laws and administrative regulations, take necessary measures to safeguard the security of the personal information they process, and assist personal information handlers in fulfilling the obligations provided in this Law.

第六章 履行个人信息保护职责的部门	**Chapter VI: Authorities Performing Personal Information Protection Duties**
第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。 县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。 前两款规定的部门统称为履行个人信息保护职责的部门。	Article 60: The State cyberspace administration is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work. Relevant authorities under the State Council are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations. County-level and higher People's Governments' relevant departments' personal information protection, supervision, and management duties and responsibilities are determined according to relevant State regulations. Authorities specified in the preceding two paragraphs shall be collectively referred to authorities performing personal information protection duties.
第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责： 开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作； （二）接受、处理与个人信息保护有关的投诉、举报； （三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果； （四）调查、处理违法个人信息处理活动； （五）法律、行政法规规定的其他职责。	Article 61: Authorities performing personal information protection duties shall perform the following personal information protection duties: 1. Conducting awareness and education activities for personal information, and guiding and supervising personal information handlers' conduct in personal information protection; 2. Accepting and processing personal information protection-related complaints and reports; 3. Organizing the testing and evaluation of the personal information protection situation within their application programs, etc., and disclosing the results; 4. Investigating and processing unlawful personal information processing activities; 5. Other duties provided in laws or administrative regulations.
第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作： （一）制定个人信息保护具体规则、标准； （二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准； （三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设； （四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务； （五）完善个人信息保护投诉、举报工作机制。	Article 62: The State cyberspace administration shall organize and coordinate relevant authorities in promoting the following personal information protection work: Formulate concrete personal information protection rules and standards; Formulate specialized personal information protection rules and standards for small-scale personal information handlers, new technologies and new applications regarding sensitive personal information, facial recognition, artificial intelligence, etc.; 3.Support the research, development, and broad adoption of secure and convenient electronic identity authentication technology, and promote the construction of public online identity authentication services; 4.Advance the construction of a socialized service systems for personal information protection, and support relevant organizations to launch personal information protection evaluation and certification services; 5.Improve the complaints and reports mechanism for personal information protection.

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：
（一）询问有关当事人，调查与个人信息处理活动有关的情况；
（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；
（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查；
（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。
履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

Article 63: An authority performing personal information protection duties may adopt the following measures when performing its personal information protection duties:

Interviewing relevant concerned parties, and investigating circumstances related to personal information processing activities;

Consulting and reproducing a concerned party's contracts, records, receipts as well as other relevant material related to personal information processing activities;

Conducting on-site inspections, and conducting investigations of suspected unlawful personal information processing activities;

Inspecting equipment and articles relevant to personal information processing activities; and when there is evidence the equipment or articles are used to engage in illegal personal information processing activities, after reporting to their department's main person responsible in writing and receiving approval, they may seal or confiscate it.

Where authority performing personal information protection duties perform their duties according to the law, concerned parties shall provide assistance and cooperation, and they may not obstruct or impede them.

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

Article 64: Where authority performing personal information protection duties discover relatively considerable risks exist in personal information processing activities or personal information security incidents occur, the authority may, in accordance with its authority and procedure as prescribed, conduct a talk with the personal information handler's legal representative or main person responsible, or require personal information handlers to entrust specialized institutions to conduct compliance audits of their personal information processing activities. Personal information handlers shall adopt measures to rectify and eliminate any hazard as required.

Where authority performing personal information protection duties discover in the course of their duties discover unlawful processing of personal information that is suspected of being involved in a crime, the authority shall promptly refer the matter to public security authorities for legal handling.

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

Article 65: Any organization or individual shall have the right to file a complaint or report about unlawful personal information processing activities with authority performing personal information protection duties. Authorities receiving complaints or reports shall process them promptly in accordance with the law, and notify the complaining or reporting person of the result.

Authority performing personal information protection duties shall publish contact information to receive complaints and reports.

第七章 法律责任	**Chapter VII: Legal Liability**
第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	Article 66: Anyone processing personal information in violation of this Law or failing to perform any obligation of personal information protection specified in this Law in the processing of personal information will be ordered to make a correction, given a warning, and confiscated of any illegal gain by the authorities performing personal information protection duties, and any application program that unlawfully processes personal information will be ordered to suspend or terminate its services; and where the correction is refused, a fine of not more than CNY 1 million will be imposed; the directly responsible person in charge and other directly responsible personnel will be fined between CNY 10,000 and CNY 100,000. Where the circumstances of the unlawful acts mentioned in the preceding paragraph are grave, the violator will be ordered to make a correction, confiscated of any illegal again, and fined up to CNY50 million, or 5% of last year's annual revenue by the authorities performing personal information protection duties at the provincial level or above; and may also be ordered to suspend any related activity or to suspend business for rectification, and/or be reported to the relevant authority for the revocation of the related business permit or the business license; and any person in charge or any other individual directly liable for the violation will be fined between CNY100,000 and CNY1 million and may also be banned for a certain period of time from serving as a director, supervisor, senior officer or personal information protection officer of a relevant enterprise.
第六十七条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。	Article 67: Any unlawful activity specified in this Law if committed shall be entered into credit files as provided by relevant laws and administrative regulations, and be disclosed to the public.
第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。 履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。	Article 68: Where any State organ fails to perform personal information protection duties as provided in this Law, its superior organ or the authorities performing personal information protection duties shall order correction; the directly responsible person in charge and other directly responsible persons are to be disciplined according to the law. Any personnel of an authority performing personal information protection duties who commits any neglect of duty, abuse of authority, or misconduct for personal gains which does not constitutes a crime shall be subject to disciplinary sanctions according to the law.
第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。 前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额	Article 69: Where any damages are caused due to an infringement of personal information rights and interests in the processing of personal information, the infringing personal information processor if unable to prove no fault on its/his/her part shall bear tort liability, including the liability for damages. The liability for damages specified in the preceding paragraph shall be determined according to the resulting loss to the individual or the gains derived by the infringing personal information handler; or the amount of damages shall be determined based on the actual situation if such losses or gains are difficult to be ascertained.

第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。	Article 70: Where personal information handlers process personal information in violation of the provisions of this Law, infringing on the rights and benefits of many individuals, the People's Procuratorates, statutorily designated consumer organizations, and organizations designated by the State cyberspace administration may file a lawsuit with a People's Court according to the law.
第七十一条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。	Article 71: Any violation of this Law that constitutes a violation of public security administration shall be subject to penalty under public security administration rules according to the law; and any such violation that constitutes a criminal offence shall be investigated for criminal liability according to the law.
第八章 附 则	**Chapter VIII: Supplemental Provisions**
第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。 法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。	Article 72: This law does not apply to processing personal information by natural persons for personal or family affairs. Where law contains provisions on personal information processing by People's Governments at all levels and relevant departments and organizations implementing statistical and archival management activities, those provisions apply.
第七十三条 本法下列用语的含义： （一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。 （二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。 （三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。 （四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。	Article 73: The following terms of this Law are defined as follows: "Personal information handler" refers to organizations and individuals that, in personal information processing activities, autonomously determine processing purposes. "Automated decision-making" refers to the use of computer programs to automatically analyze or assess individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status, etc., and engage in decision-making activities. "De-identification" refers to the process of personal information undergoing processing to ensure it is impossible to identify specific natural persons without the support of additional information. 4."Anonymization" refers to the process of personal information undergoing processing to make it impossible to distinguish specific natural persons and impossible to restore.
第七十四条 本法自2021年11月1日起施行。	Article 74: This Law shall enter into force on November 1, 2021.

ABOUT DENTONS

Dentons is the world's largest law firm, connecting top-tier talent to the world's challenges and opportunities with 20,000 professionals including 12,000 lawyers, in more than 200 locations, in more than 80 countries. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and award-winning client service challenge the status quo to advance client interests.

dentons.com

CSBrand-67015-Dentons Guide to China Personal Information Protection Law — 25/08/2021