大成 DENTONS

# Stricter than the GDPR, China's Privacy Law Provides Prohibitive and Control Obligations

September 2021

## Introduction

On August 20, the Chinese legislature passed the *Personal Information Protection Law* ("PIPL"). Consisting of eight chapters and 74 articles, the PIPL provides comprehensive provisions that give stronger legal assurance in the realm of privacy protection. These provisions include rules on the scope of application and personal information processing, on cross-border transmission, subject persons' rights in processing activities, personal information processors' obligations, as well as on regulatory authorities and penalties.

This new law sets out tougher compliance obligations than its European and US peers on how companies can collect and handle personal information, and could have a great impact on the way Chinese and non-Chinese businesses operate. This article provides an overview of the PIPL in an attempt to help enterprises understand 1) what are the new corporate compliance obligations created by the PIPL; 2) how to take appropriate control measures; and 3) how to adjust internal compliance plans in a timely way to manage compliance risks.

The PIPL has the following notable features:

- Interrelationship with other laws, with the Constitution as the legislative basis;
- Clearly set boundaries for the processing of personal information;
- Interrelationship with other laws, with the Constitution as the legislative basis;
- Clearly set boundaries for the processing of personal information;
- Informed or withdrawable consent is a right and an obligation;
- Strengthened protection of minors' personal information;
- Tightened protection of sensitive personal information;
- Clarified scope of sensitive personal information;
- Demystified compliance obligations of personal information processors;
- Practical cross-border transfer of personal information;
- Heightened regulation and punitive measures.

## Interrelationship with other laws, with the Constitution as the legislative basis

With the *Constitution* as the legislative basis, the PIPL inherits the relevant provisions of the *Cyber Security Law of the People's Republic of China* (hereinafter referred to as the "Cyber Security Law") and the *Civil Code of the People's Republic of China* (hereinafter referred to as the "Civil Code") on the protection of personal information, and it elaborates on their rules and requirements.

Articles 38 and 40 of the *Constitution* clearly provide for the protection of citizens' personal dignity and the freedom and confidentiality of correspondence. Especially in relation to the *Constitution*, Article 1 of the PIPL states that this Law is enacted in accordance with the *Constitution* in order to protect personal information rights and interests, regulate personal information processing activities and promote rational use of personal information. Evidently, affording constitutional status to persons in relation to personal information proves that China takes the protection of personal information very seriously.

Therefore, with the *Constitution* as the legal basis, the protection of personal information becomes a multi-dimensional mission:

- Personal dignity and the freedom and confidentiality of correspondence are treated as a matter of human rights;
- The protection of civil interests and rights can be claimed via the courts; and
- Administrative organizations are committed to protecting public interests (Article 11), and the People's Prosecuting Institutions, consumer organizations and the state internet information department may bring a public-interests lawsuit (Article 70).

Certainly, China's constitutional law does not have teeth as sharp as that of some other jurisdictions (like the US); however, the correlation of personal information with human rights showcases the determination of China to protect personal information to the highest extent.

## Clearly set boundaries for the processing of personal information

Articles 5 through 10 set clear boundaries as principles for the processing of personal information:

| Articles | Prohibitive principles | Control principles |
|---|---|---|
| **Article 5** | PI shall not be processed by means of deception, fraud, coercion, etc. | The principles of legality, justness, necessity and good faith shall be followed in the processing of PI. |
| **Article 6** | PI shall not be collected excessively. | The processing of PI shall have a clear and reasonable purpose, be directly related to the processing purpose, and adopt the method that has the least impact on personal rights and interests.<br><br>The collection of PI shall be limited to the minimum range for the purpose of processing. |
| **Article 7** | | In handling PI, the principles of openness and transparency shall be followed, the rules for handling PI shall be disclosed, and the purpose, method and scope of processing shall be clearly stated. |
| **Article 8** | | The quality of PI shall be guaranteed to avoid adverse effects on personal rights and interests due to inaccurate and incomplete PI. |
| **Article 9** | | A PI processor shall be responsible for its PI processing activities and take necessary measures to ensure the security of the PI processed. |
| **Article 10** | No organization or individual may illegally collect, use, process or transmit other people's PI, or illegally buy, sell, provide or disclose other people's personal information; it shall not engage in personal information processing activities endangering national security and public interests. | |

Article 6 stipulates that the processing of personal information shall 1) have a clear and reasonable purpose; 2) be directly related to the purpose of processing; and 3) be processed in a way that minimizes infringement of individual rights and interests. Collection of personal information shall be limited to the minimum scope for the purpose of processing. This provision echoes with Article 1035 of the Civil Code, "the handling of personal information shall follow the principles of legality, legitimacy and necessity, and shall not be excessively processed". In practice, it is critical for app operators to determine the "minimum scope for processing purposes" for this provision. To this end, reference should be made to the *Regulations on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications* (hereinafter referred to as the "Provisions on the Scope of Necessary Personal Information") that were issued in March this year.

The Provisions on the Scope of Necessary Personal Information explained the personal information necessary for the basic functions of different types of apps, as well as what services were required for the app to function properly. For example, the basic function of job-hunting apps is "job-hunting information exchange", as part of which they collect necessary personal information including registered users' mobile phone numbers and resumes provided by job seekers. This corresponds to the personal information that is "necessary for the performance of a contract in which an individual is a party" as stipulated in Article 13 of the PIPL. During the operation of apps, enterprises should, in accordance with the Provisions on the Scope of Necessary Personal Information, specify the scope of personal information that must be collected to provide basic functions and services, and communicate in a timely way with business departments to adjust the scope of personal information actually collected to ensure that the requirements of the PIPL are met.

However, for other apps and other forms of products (such as websites and PC terminals) that are not within the scope of 39 categories stipulated in the Provisions on the Scope of Necessary Personal Information, strict evaluation should be conducted when collecting personal information to avoid collecting and using personal information beyond the necessary scope.

Additionally, in order to prevent personal information leakage and prevent harm to national security, Article 10 also clearly stipulates that any organization or individual shall not illegally collect, use, process, transmit other people's personal information; shall not illegally trade, provide or disclose other people's personal information; and shall not engage in personal information processing activities that endanger national security and public interests. This point is also consistent with Article 111 of the Civil Code, reflecting the compatibility between the PIPL and the Civil Code in this area.

## personal information is balanced with exceptions

To obtain personal consent is the basis for the processing of personal information (Article 13.1). However, the PIPL provides for the following exceptions where there is no necessity to obtain personal consent:

- Necessary for the conclusion and performance of the contract to which the individual is a party, or for the implementation of human resources management in accordance with the labor rules and regulations formulated according to law and the collective contract signed according to law (Article 13.2).
- Necessary for the performance of legal duties or legal obligations (Article 13.3).
- Necessary for responding to public health emergencies or protecting the life, health and property of natural persons in emergencies (Article 13.4).
- To implement news reporting, public opinion supervision and other acts for the public interest, and deal with personal information within a reasonable range (Article 13.5).
- To handle, within a reasonable scope, the personal information disclosed by individuals themselves or other legally disclosed personal information in accordance with the provisions of this law (Article 13.6).
- Other circumstances stipulated by laws and administrative regulations (Article 13.7).

Compared with the previous draft versions, an additional content exception is added, that is the second part of Article 13.2, "it is necessary to implement human resource management in accordance with labor rules and regulations formulated according to law and collective contracts signed according to law". This change balances employers' need for legitimate use of workers' personal information collected/accessed in the course of their work with employees' need for the protection of their personal information.

In this regard, enterprises should evaluate and analyze the necessity of collecting employees' personal information in the workplace, especially whether the collection and use of employees' personal information is necessary for human resource management in such scenarios as monitoring employees in the workplace, conducting background checks before employees are hired, and even using some software in monitoring employee fraudulent actions. In practice, the necessity could be justified by the labor manuals, or the collective contracts formulated according to law.

# Informed or withdrawable consent is a right and an obligation

Informed or withdrawable consent is the right of a subject person, and an obligation of a personal information processor.

| Rights of subject person | Compliance obligations | |
|---|---|---|
| | **Prohibitive** | **Control** |
| The consent shall be made voluntarily and clearly by the individual on the premise of full knowledge (Article 14). | A personal information processor shall not refuse to provide products or services on the grounds that an individual does not agree to process his personal information, except where processing of personal information is necessary for the provision of products or services (Article 16). | Before processing personal information, a personal information processor shall truthfully, accurately and completely inform the individual of the following matters in a conspicuous manner and in a clear and understandable language:<br>(1) The name or contact information of the personal information processor;<br>(2) The purpose and method of personal information processing, the type of personal information processed and the storage period;<br>(3) Ways and procedures for individuals to exercise their rights under this law;<br>(4) Other matters that shall be notified according to laws and administrative regulations.<br><br>Where the matters specified in the preceding paragraph are changed, the individual shall be informed of the changed part.<br><br>Where a personal information processor notifies the matters specified in paragraph 1 by formulating personal information processing rules, the processing rules shall be open and easy to consult and preserve (Article 17). |
| An individual has the right to withdraw his consent if the processing of personal information is based on the individual's consent (Article 15). | A personal information processor shall not refuse to provide products or services on the grounds that an individual withdraws his consent, except where processing of personal information is necessary for the provision of products or services (Article 16). | The personal information processor shall provide a convenient way to withdraw consent (Article 15). |

## Strengthened protection of minors' personal information

In recent years, the state attaches more and more importance to the protection of personal information of children (i.e., minors under the age of 14). As such, China promulgated the *Minors Protection Law*, *Children's Personal Information Network Protection Regulations*, etc.

It is made clear that information processors also need to follow the legality, legitimacy and necessity principles, and should obtain the consent of the children's parents or other guardians in processing children's personal information through the network. Such a requirement is undoubtedly incorporated into the texts of the PIPL. However, it is worth paying attention to the fact that, according to research, there are certain practical obstacles in the mechanism of "verifying parental consent" in almost all mainstream apps in China.

Appendix A of the "*Guidelines on Information Security Technology Personal Information Notification and Consent* (Draft for Public Opinion)" elaborated the methods of identity verification for minors and their guardians and points out that the essential differences of different products and/or services should be fully considered in the verification, so as to reduce unnecessary interruptions for users.

For mobile phone bank, auto financing, and other products, because the probability of participation of minors is low, questions like whether you are over 14 can be raised through a popup window. As for social networking products such as games and live broadcasts, heightened verification methods should be adopted, such as input of the birth date, ID number and other ways for the guardian to monitor their activities. To this end, companies can refer to overseas practices on such matters. For example, the *Children's Online Privacy Protection Act* (hereinafter referred to as "COPPA Act") enacted by the United States requires parents to give consent to the collection, use and public disclosure of children's personal information, and requires network operators to inform parents how to express consent through corresponding mechanisms. The COPPA provides several ways for obtaining verifiable consent from a guardian, such as by sending a verifiable email to the parent or by telephone.

What companies need to pay special attention to is that the PIPL clearly identifies children's personal information as sensitive personal information. Such personal information should be handled with the consent of the minor's parents or other guardians, and special personal information processing rules should be formulated.

This rule is consistent with the provisions of the *Protection of Children's Personal Information Regulation*, which also places emphasis on the protection of minors' personal information on the legal level. Therefore, when collecting and using the personal information of minors, companies should be aware that in addition to the requirements on the protection of minors' personal information, they also need to meet the requirements on the processing of sensitive personal information. For example, personal information processors should conduct a risk assessment and also record the data processing before processing sensitive personal information.

## Tightened protection of sensitive personal information

The PIPL provides for various rules for the protection of personal information. A noteworthy feature is that the retention period of personal information shall be the shortest time necessary to achieve the purpose of processing (Article 19).

The PIPL has tightened the protection of sensitive personal information—the processing of sensitive personal information may only proceed with a specific purpose, sufficient necessity, and with strict protection measures (Article 28). Under the PIPL, sensitive personal information is biometric information, religious beliefs, specific identity, medical and health information, financial account information, tracking information and personal information of minors under the age of 14.

Additionally, Article 26 of the PIPL has special provisions in response to the public concern over facial recognition technology. Relevant state regulations should be observed, and prominent public signs should be placed where there are face recognition and personal information collection devices in the public realm. The collected personal images and identification information shall only be used for the purpose of maintaining public safety and shall not be used for other purposes except where personal consent has been obtained.

At the end of July 2021, the Supreme People's Court formulated and published the *Provisions of the Supreme People's Court on several Issues concerning the Application of the Law to the Trial of Civil Cases Involving the Use of Facial Recognition Technology in Handling Personal Information* (hereinafter referred to as the "Facial Recognition Provisions"), which made clear that the use of facial recognition technology in public places should comply with relevant laws and regulations.

The first paragraph of Article 2 of the Facial Recognition Provisions stipulates that "using face recognition technology for face verification, identification or analysis in hotels, shopping malls, banks, railway stations, airports, sports venues, entertainment venues and other business sites or public places in violation of laws and administrative regulations" is an act infringing upon the personality rights and interests of natural persons.

In this regard, companies should be cautious if they are collecting facial information for the purpose of maintaining public safety. If facial information is collected for purposes other than maintaining public safety, consent from the subject of personal information should be obtained and a series of relevant rules for processing facial information should be observed.

If it is done for other purposes, the purpose, method and scope of the collection and use of facial information should be clearly stated.
For example, in public places where cameras are installed, a sign should be put up stating the purposes for such installation and what it is. For example, a sign may state that "we promise to protect your facial and other information security, and you can consult the front desk or scan the QR code for details". On the other hand, companies should obtain the express consent of the subject person for collecting personal information and ensure that the express consent is made independently on the basis of full knowledge.

## Clearly specified rights of subject persons

The PIPL specifies the rights of subject persons as follows:

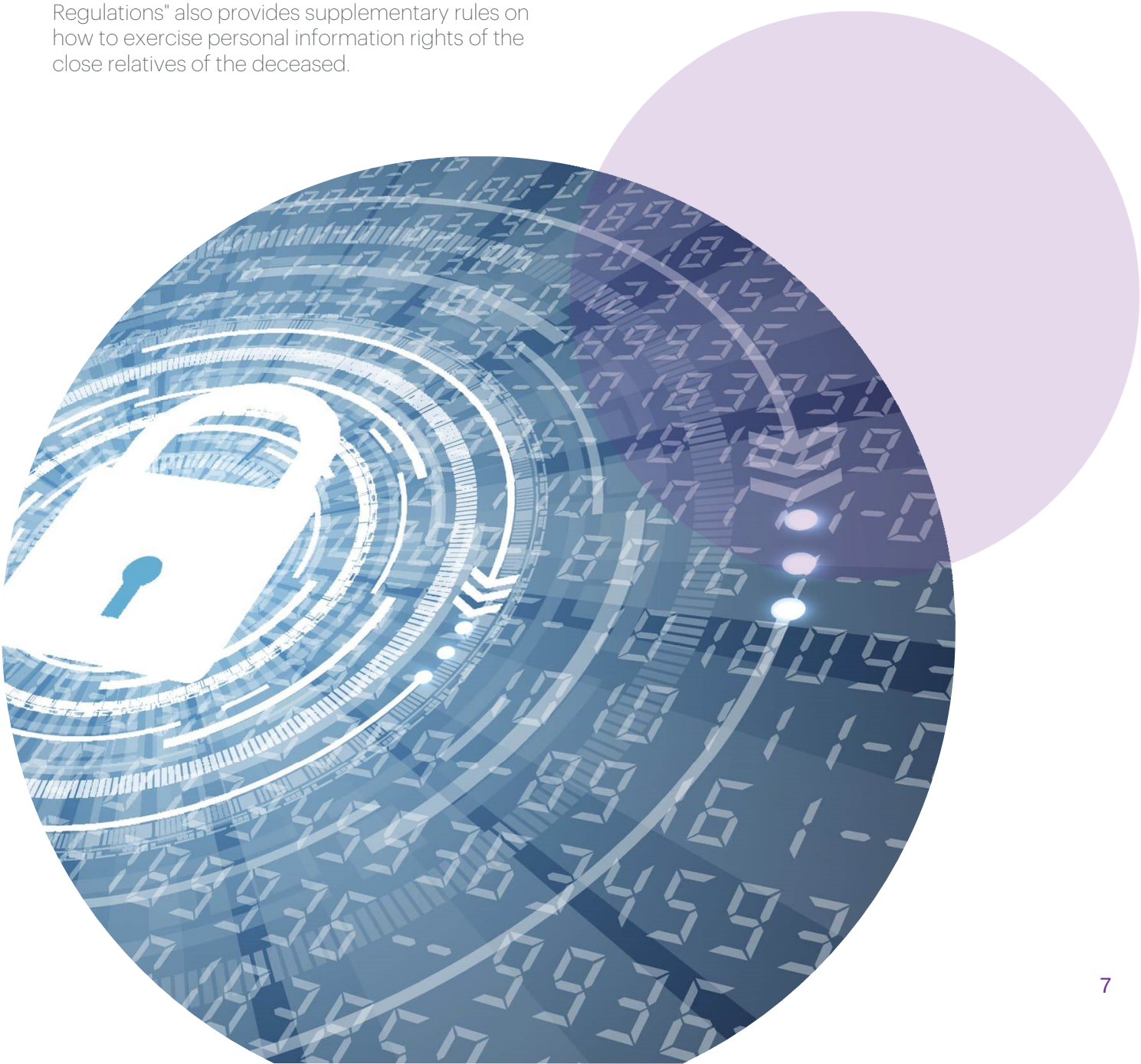
| Rights of subject person | Compliance obligations of PI processors | |
|---|---|---|
| | Prohibitive | Control |
| - The right to know and decide on the processing of PI.<br>- The right to restrict or refuse others to process PI (Article 44). | | |
| - The right to consult and copy PI from a PI processor (Article 45). | | PI processor shall provide it in a timely manner (Article 45). |
| - The right to transfer PI to a designated PI processor (Article 45). | | The PI processor shall provide a way of transfer (Article 45). |
| - The right to request a PI processor to correct or supplement PI (Article 46). | | The PI processor shall verify PI and correct errors or supplement PI in time (Article 46). |
| - The right to request deletion (Article 47). | | Under any of the following circumstances provided in Article 47, the personal information processor shall take the initiative to delete the personal information; if the personal information processor does not delete, the individual has the right to request deletion (Article 47). |
| - The right for the explanation of PI processing rules (Article 48). | | |
| - The right of the close relatives of the deceased (Article 49). | | If a natural person dies, his close relatives may, for their own legitimate and legitimate interests, exercise the rights of consulting, copying, correcting and deleting the relevant personal information of the deceased unless otherwise arranged by the deceased before his death (Article 49). |
| - The right to sue: if a personal information processor refuses an individual's request to exercise his rights, the individual may bring a lawsuit to the People's Court according to law (Article 50). | | A personal information processor shall establish a convenient application acceptance and processing mechanism for individuals to exercise their rights. If a personal information processor refuses to exercise the requests of a subject person, the processor shall state its reasons (Article 50). |

Article 49 of the PIPL stipulates the personal information rights and interests of the close relatives of the deceased. The close relatives of the deceased may, for their own lawful and legitimate interests, exercise the rights of consulting, copying, correcting and deleting the relevant personal information of the deceased as stipulated in Chapter 4, unless the deceased had otherwise arranged before his death. The provision is in line with Article 994 of the Civil Code, which also provides that the spouse, children, parents or close relatives of the deceased have the right to claim civil liability under the law when the privacy of the deceased is violated, but relevant specific rules for exercising this right have been absent up until now.

The PIPL has defined the scope of personal information rights of the close relatives of the deceased (for example, the rights to access, copy, correct, delete and other personal information of the deceased can be exercised by the close relatives of the deceased). At the same time, Article 15 of the recently promulgated "Facial Recognition Regulations" also provides supplementary rules on how to exercise personal information rights of the close relatives of the deceased.

In addition, the PIPL also improves the personal information protection complaint reporting mechanism. Article 59 requires personal information processors to establish a "convenient" mechanism for applying to exercise rights. If the personal information processor refuses individuals' requests, the individual may file a lawsuit in a people's court according to law. In addition, according to Article 61, the departments responsible for protecting personal information are responsible for receiving and handling complaints and reports related to the protection of personal information.

Finally, Article 64 stipulates that the department that performs the duty of personal information protection shall promptly transfer the case to the public security authorities according to law if it spots criminal activities in the course of performing its duty.



# Demystified compliance obligations of personal information processors

Chapter 5 provides for the compliance obligations of a personal information processor.

| Compliance Obligations | |
|---|---|
| **Prohibitive** | **Control** |
| | The obligation to prevent unauthorized access, disclosure, tampering and loss of PI. According to the processing purpose, processing method, types of personal information, impact on personal rights and interests and possible security risks of PI, the processor must:<br>(1) Formulate internal management system and operating procedures;<br>(2) Implement classified management of PI;<br>(3) Take corresponding security technical measures such as encryption and de-identification;<br>(4) Determine the operation authority of PI processing, and regularly carry out safety education and training for employees;<br>(5) Formulate and organize the implementation of emergency plans for PI security incidents;<br>(6) Carry out other measures stipulated by laws and administrative regulations (Article 51). |
| | The obligation of designating the PIP (personal information protector).<br>If the amount of PI processed reaches the amount specified by the national network information department, the PI processor shall designate the person in charge of PI protection to supervise the PI processing activities and the protection measures taken (Article 52). |
| | The obligation of a non-Chinese PI processor to set up a special agency or designated representative in China. A PI processor outside China shall set up a special agency or designated representative within China to handle matters related to PI protection and submit the name of the relevant agency or the name and contact information of the representative to the department performing the responsibility of PI protection (Article 53). |
| | The obligation of audit. A PI processor shall regularly audit its compliance with laws and administrative regulations in handling personal information (Article 54). |
| | The obligation to conduct a PI protection impact assessment. Under any of the following circumstances, the PI processor shall conduct a PI protection impact assessment in advance and record the processing:<br>(1) Where the processor handles sensitive personal information;<br>(2) Where it uses personal information for automatic decision-making;<br>(3) When it entrusts the processing of personal information, provides personal information to other personal information processors, and discloses personal information;<br>(4) When it send personal information abroad;<br>(5) For other personal information processing activities that have a significant impact on personal rights and interests (Articles 55 & 56). |
| | The obligation of remodifying and reporting to authority. Where personal information is leaked, tampered with or lost, the personal information processor shall immediately take remedial measures and notify the department and individual performing the responsibility of personal information protection (Article 57). |
| | The obligation of notifying individuals. If a PI processor takes measures to effectively avoid harm caused by information disclosure, tampering and loss, the PI processor need not notify the individual; if the department performing the duty of PI protection considers that it may cause harm, it has the right to require the PI processor to notify the individual (Article 57). |
| | Extra obligations of an important internet platform service provider. A PI processor that provides important internet platform services, has a large number of users and complex business types shall perform some extra obligations as provided in Article 58. |
| | The obligation of a trustee for assistance. A trustee entrusted to process PI shall take necessary measures to ensure the security of the personal information processed and assist the personal information processor in performing its obligations under this law (Article 59). |

The personal information processors that provide basic internet platform services which are subject to Article 58 are often in possession of a large amount of user data, and their compliance is a matter of the public interest. Considering that such entities are generally large in size and occupy a very large share of the market, the supervision by external institutions can better regulate the platform's behavior for compliance purposes. Article 58, Paragraph 1 of the PIPL also added that large internet platforms should "establish and improve the compliance system for personal information protection in accordance with national regulations". The second paragraph added the principles of openness, fairness and justice to be reflected in the rules of the platform, thereby clarifying the standards of processing personal information and the obligations of the product or service providers in this regard.

As a result, affected entities should establish and improve their internal data compliance systems and make internal provisions on the company's compliance obligations in the process of personal information collection, storage, use, sharing, transfer, public disclosure and deletion in accordance with laws and regulations and based on the life cycle of personal information. Personnel involved should strictly observe companies' regulations in this regard and keep records for regulatory purposes. Companies also need to formulate the platform rules, such as the platform service agreement, trading rules, etc., to define the product or service provider's norms for handling personal information and its obligations to protect personal information.

For example, operators in online trading platforms shall keep the personal information they collect strictly confidential, and shall not provide it to any third party, including affiliated parties, without the authorization and consent of the collected person, except for cooperating with supervision and law enforcement activities according to law.

## Practical cross-border transfer of personal information

Chapter 3 of the PIPL specifically provides a set of rules for the cross-border movement of personal information. Article 38 provides that where international treaties or agreements concluded or acceded to by the People's Republic of China have provisions on the conditions for providing personal information outside China, such provisions may apply.

necessary measures to ensure that the overseas receiving party's personal information processing activities meet the protection standards stipulated in this law. Therefore, when carrying out cross-border data transmission activities, companies should ensure that overseas recipients have an adequate level of personal information protection.

Since there is no detailed high-level legal rule on outbound data in China at present, the specific standards can be appropriately referred to the relevant provisions of the *Measures for the Security Assessment of Outbound Personal Information* (a draft for comment).

First of all, both parties shall specify in the contract signed with the overseas receiving party the purpose, type and retention period of personal information leaving the country and make it clear that the overseas receiving party can fully protect the legitimate rights and interests of the personal information subject. At the same time, the receiving party shall: (1) provide the personal information subject with access to its personal information; (2) use personal information for the purposes agreed herein, and the retention period of personal information abroad shall not exceed the time limit agreed herein; (3) confirm that the signing of the contract and the performance of contractual obligations will not violate the legal requirements of the recipient's country.

In case of any change in the legal environment in the country or region where the recipient is located that may affect the execution of the contract, the recipient shall notify the personal information processor in a timely manner and report to the provincial network information department where the network operator is located through the personal information processor.

In addition, Article 41 of the PIPL provides that the competent authorities of China shall handle requests from foreign judicial or law enforcement agencies for the provision of personal information stored in China in accordance with relevant laws and international treaties or agreements concluded or acceded to by China, or in accordance with the principle of equality and reciprocity.

Without the approval of the competent authorities of China, personal information processors shall not provide personal information stored in China to foreign judicial or law enforcement agencies. It is stipulated that when overseas judicial or law enforcement agencies request to be provided with domestic personal information, the personal information processor shall only provide it with the approval of the competent authorities of China. This point is basically consistent with the provisions of Article 36 of the *Data Security Law*, but there are no detailed provisions on the competent authority and approval process stipulated in this article, which need to be further explained by subsequent legislation or regulations.

## Heightened regulation and punitive measures

Compared with the PIPL's second draft, the PIPL's Article 61 provides an additional responsibility for departments that are responsible for protecting personal information, namely to organize the evaluation of the protection of personal information such as applications and publish the evaluation results. Additionally, according to Article 62, the internet and information department can formulate rules on personal information protection for small information processors. They can further construct public services on network identity authentication and reporting mechanisms for the protection of personal information, thereby shedding light on future regulatory trends.

As for punitive measures, the PIPL's Article 66 provides two categories of penalties. The first is to order apps that illegally handle personal information to cease provisions of products and services. Secondly, for serious violations, the directly responsible executives and other directly responsible personnel can be banned from serving as directors, supervisors, senior managers and persons in charge of personal information protection for a certain period of time in addition to fines.

However, the PIPL did not elaborate on what constitutes a serious violation. If reference is made to GDPR cases, data breaches or the number of data subjects affected may play a big role in this regard. It is always good practice for companies to take proactive remedial measures so as to be treated leniently by the regulator. Additionally, the PIPL stipulated fines of up to CNY 50 million (US$7.35 million) or up to 5 percent of the previous year's turnover. It is for this reason that companies need to be proactive in their compliance endeavors.

Article 68 of the PIPL also stipulates that the personnel of the department performing the duty of personal information protection shall be punished in accordance with the law if they neglect their duties, abuse their power, or engage in malpractice for personal gain, which does not constitute a crime.

This strengthens the responsibilities of administrative supervision departments. Regulators should not only perform their personal information supervision duties in accordance with external laws and regulations, but also pay attention to the normative behavior of public officials and the requirements of the administrative system, so as to curb the infringement of citizens' personal information from within the system.

Notably, where a personal information processor processes personal information in violation of the provisions of this law and infringes upon the rights and interests of individuals, the People's Prosecuting Institute, consumer organizations prescribed by law and organizations determined by the state internet information department may bring a lawsuit to the People's Court (Article 70).

Please also bear in mind whenever there is a violation of Criminal Law, criminal liabilities could be triggered.

## Concluding Thoughts

The PIPL creates a comprehensive legal regime for personal information protection under the Constitution, criminal law, civil law and administrative law. Especially, the law provides for the rights for subject persons, and obligations for personal information processors. Non compliances could trigger civil, administrative and/or criminal liabilities. Notably, multinational companies and non-Chinese companies from outside China could be subject to this law too as a personal information processor or have the duties not to infringe the personal information of subject persons from within China. Because violators could be subject to heavy penalties (including business disruption and criminal liabilities), there is no reason for anyone to downplay or even neglect the PIPL and its compliance obligations.

# Key Contact

**Henry Chen (陈立彤)**
Senior Partner, Shanghai
D +86 21 2028 3821
E henry.chen@dentons.cn

**www.dentons.com**