China Insight

PRC Promulgated Personal Information Protection Law

Dear Sir or Madam,

Adopted by the Standing Committee of National People's Congress on 20 August 2021, the *PRC Personal Information Protection Law* ("PIPL") will take effect as of 1 November 2021. It is the first comprehensive and specialized legislation regarding personal information protection in China. Please find below a brief of the PIPL.

Kind regards,
CMS, China

Adopted by the Standing Committee of National People's Congress on 20 August 2021, the *PRC Personal Information Protection Law* ("PIPL") will take effect as of 1 November 2021.

1. Background

The PIPL is the first comprehensive and specialized legislation regarding personal information protection in China. The concept of personal information protection was first incorporated into the *PRC Cybersecurity Law*, but was limited to the personal information handled via networks. The *PRC Civil Code* later recognized personal information as a fundamental personal right and established general rules for personal information protection. The first draft of the PIPL was published in October 2020, the second draft came out in April 2021 and the final PIPL was adopted shortly after another four months on 20 August 2021. The PIPL sets up detailed rules for handling personal information and raises new challenges for enterprises when handling personal information. As the fundamental legislation for personal information protection, the PIPL aims to safeguard individuals' personal information at a new level.

2. Key Aspects in the PIPL

The PIPL consists of the following eight chapters and seventy-four articles in total. As the PIPL incorporates detailed rules in various aspects, we will introduce highlights of each chapter following the structure of the PIPL.

- General provisions
- Rules for handling personal information
- Specific rules for handling sensitive personal information
- Rules for cross-border transfer of personal information
- Rights of individuals in personal information handling activities
- Obligations of personal information handlers

– Authorities performing personal information protection duties

– Legal liabilities for violation

3. General Provisions

The general provisions clarify the definition of personal information and personal information handling activities and also establish extraterritorial jurisdiction of the PIPL. In addition, the general provisions set up basic principles for handling personal information.

a) Definitions

Article 4 of the PIPL defines that personal information refers to any kind of information related to an identified or identifiable natural person which is recorded in electronic form or other manners, excluding anonymized information. Article 73.4 of the PIPL further clarifies that anonymization refers to the process in which any personal information is handled to the extent that it cannot identify a specific natural person and cannot be restored to its original state.

Further, Article 4 of the PIPL defines that personal information handling activities include the collection, storage, use, processing, transfer, provision, disclosure, and deletion of personal information, while personal information handling activities conducted by natural persons due to their personal or family affairs are not subject to this law according to Article 72.

b) Extraterritorial jurisdiction

The PIPL establishes extraterritorial jurisdiction of personal information handling activities in overseas countries. In addition to personal information handling activities carried out within the territory of the PRC, Article 3 of the PIPL clearly provides that it shall also apply to any personal information handling activities carried out outside the territory of the PRC 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 the PRC;

(2) Where the purpose of the activity is to analyze or assess the behavior of that natural person located within the PRC; or

(3) Any other circumstance as provided by laws or administrative regulations.

Further according to Article 53 of the PIPL, if the overseas personal information handling activity falls into the above scope of extraterritorial jurisdiction, the personal information handler outside the territory of the PRC shall establish a special agency or appoint a representative within the territory of the PRC to be responsible for personal information protection-related affairs, and submit the name of such agency or the name and contact information of the representative to the relevant authorities performing personal information protection duties.

c) Basic principles

The PIPL stipulates the basic principles for handling personal information as follows.

(1) Article 5 of the PIPL states that in handling personal information, the principles of legality, fairness, necessity and good faith must be observed.

(2) Article 6 of the PIPL states that the principles of specificity and relativeness must be observed, and provides that handling personal information shall have a specified and reasonable purpose and shall be conducted in a manner which is directly relevant to the purpose and has the least impact on personal rights and interests. In addition, collection of personal information shall be limited to the minimum scope necessary for achieving the purpose and shall not be excessive.

(3) Article 7 of the PIPL states that the principles of openness and transparency must be observed, and provides that rules of personal information handling shall be disclosed and the purpose, method and scope of such handling shall be expressly stated.

(4) Article 8 of the PIPL states that the principles of integrity and accuracy shall be observed, and provides that the quality of personal information shall be ensured in order to avoid any negative impact on personal rights and interests due to any inaccuracy or non-integrity of the handled personal information.

(5) Article 9 of the PIPL refers to the principle of security guarantee, and provides that personal information handlers shall be responsible for their handling of personal information and take necessary measures to ensure the security of the handled personal information.

These basic principles provide general guidance on personal information handling activities and are implemented through the detailed rules in the PIPL.

4. Rules for Handling Personal Information

a) Lawful basis for handling personal information

According to the CSL, obtaining consent from personal information subjects is the prerequisite for handling personal information. Article 13 of the PIPL additionally provides the following exceptional lawful basis other than obtaining consent from personal information subjects:

(1) 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 a legally formulated employment policy or a legally concluded collective contract;

(2) Where it is necessary for performing a statutory responsibility or statutory obligation;

(3) 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;

(4) Where the personal information is handled within a reasonable scope to carry out any news reporting, supervision on public opinions or any other activities for public interest;

(5) Where the personal information, which has already been disclosed by the individual or otherwise legally disclosed, is handled within a reasonable scope and in accordance with the PIPL; or

(6) Any other circumstance as provided by laws or administrative regulations.

Compared with the second draft of the PIPL, Article 13 of the PIPL makes two important amendments as follows:

(1) The PIPL adds the new exceptional circumstance where it is necessary for carrying out human resources management under a legally formulated employment policy or a legally concluded collective contract, which is relevant to collection of employees' personal information. The PIPL states that if the relevant employees' personal information satisfies the exceptional circumstance, handling these employees' personal information may not need the consent from employees in practice.

(2) The PIPL clarifies that personal information can be handled within a reasonable scope without obtaining consent, if the personal information has already been disclosed by the individual or otherwise legally disclosed. This is consistent with Article 1036 of the *PRC Civil Code*, which provides that a personal information handler shall not be subject to civil liability, if the personal information is handled reasonably and has already been disclosed by the individual or otherwise legally disclosed, unless the personal information handling activity has been expressly refused by the individual or infringed upon the individual's significant interests.

Further, according to Article 27 of the PIPL, the exceptional circumstance as stated in the preceding paragraph shall apply unless such personal information handling activity has been expressly refused by the individual. If the handling of any disclosed personal information of an individual has a material impact on the individual, the personal information handler shall obtain consent from the individual in accordance with the PIPL. However, the PIPL has not provided further clarification on what constitutes material impact for the time being.

b) Notification and consent requirements

(1) Certain contents of the notification

As stated above, obtaining consent from the individual is the general rule for handling personal

information without exceptional circumstances. For obtaining such individual consent, notification of certain contents shall be made to the individuals. Article 17 of the PIPL provides that the personal information handler shall notify the individual of the following matters accurately and completely in a conspicuous, clear and easy-to-understand manner:

– The name and contact information of the personal information handler;

– The purpose, method, type and retention period of the personal information to be handled;

– The way and procedure for the individual to exercise his/her rights under the PIPL; and

– Any other matter to be notified as required by laws or administrative regulations.

If there is any change to the matters stated above, it shall also be notified to the individual. Article 17 of the PIPL also provides that where personal information handlers notify the above matters through their formulated personal information handling rules, such rules shall be made available to the public and easy to access and store. In practice, many enterprises make such notification through their personal information protection policy. As stated by the PIPL, such personal information protection policy should be published, such as being posted on the website.

(2) Exceptions without notifications

Article 18 of the PIPL provides exceptions for the notification requirement as stipulated under Article 17. If the relevant matters shall be kept confidential or are not required to be disclosed according to laws or administrative regulations, the personal information handler may be allowed not to make the notification as stated under Article 17.

c) Handling activities involving multiple processors

The PIPL stipulates rules for personal information handling activities involving more than one personal information handler under different circumstances as follows.

(1) Article 20 of the PIPL refers to the circumstance where two or more personal information handlers jointly handle the personal information.

In this case, the personal information handlers shall jointly decide on the purpose and method of personal information handling activities and agree on their respective rights and obligations. However, such agreement shall not affect the right of individuals to exercise their rights provided for by the PIPL against any of the personal information handlers. In addition, the above personal information handlers shall be liable jointly and severally for any damages caused due to infringement upon personal information rights and interests.

(2) Article 21 of the PIPL refers to the circumstance where a personal information handler entrusts another party for handling personal information.

In this case, the two parties shall agree on the purpose, period, and method of the entrusted handling, the type of personal information to be handled, any protection measure to be taken, and the rights and obligations of both parties, etc., and the entrusting party shall supervise the personal information handling activities carried out by the entrusted party.

The entrusted party shall handle personal information as agreed, and shall not handle personal information beyond the agreed purpose and method of the entrusted handling. If the agreement of entrusted handling fails to become effective, becomes null and void, or is cancelled or terminated, the entrusted party shall return the personal information to the entrusting personal information handler or delete it, and shall not retain such information. Without the approval of the entrusting personal information handler, the entrusted party shall not sub-entrust the handling of personal information to any other party.

Further, according to Article 59 of the PIPL, the entrusted party shall take any necessary measures to protect the security of the handled personal information as required by the PIPL and any relevant laws or administrative regulations, and assist the entrusting personal information handler in performing the obligations specified in the PIPL.

(3) Article 22 of the PIPL refers to the circumstance where a personal information handler needs to transfer personal information due to a merger, division, dissolution, declared bankruptcy or any other reasons.

In this case, the personal information handler shall inform the individual of the name and contact information of the receiving party. The receiving party shall continue to perform obligations as a personal information handler. For any change of the original purpose or method of personal information handling activities, the receiving party shall obtain consent from the individual again in accordance with the PIPL.

(4) Article 23 of the PIPL refers to the circumstance where a personal information handler provides the personal information to another personal information handler.

In this case, the personal information handler shall inform the individual of the name and contact information of the receiving party, the purpose and method of the handling, and the type of personal information handled, and obtain separate consent from the individual. The receiving party shall handle the personal information received within the scope of such purpose and method as well as type of personal information. For any change of the original purpose or method of personal information handling activities, the receiving party shall obtain consent from the individual again in accordance with the PIPL.

d) Automated decision-making

Given the dynamic application of automated decision-making for business purposes by enterprises, the PIPL stipulates specific requirements in this regard. According to Article 24 of the PIPL, where personal information is used by personal information handlers in automated decision-making, the personal information handlers shall ensure the transparency of the decision-making and a fair and impartial result. In addition, unreasonable and differential treatment of individuals in terms of transaction prices or other transaction terms shall not be implemented.

If a personal information handler conducts business marketing or information push services towards an individual by means of automated decision-making, an option not targeting at personal characteristics of the individual or an easy way to refuse to receive such business promotion shall be provided to the individual.

Further, if a decision made by a personal information handler through automated decision-making has a material impact on an individual's rights and interests, the individual shall have the right to demand the personal information handler to provide an explanation, as well as the right to refuse the decision-making by the personal information handler solely by means of automated decision-making.

e) Collection of personal images and identification information in public areas

Nowadays, image capturing devices and personal identification equipment are widely used nowadays, which raises public concerns about security of relevant personal information. Article 26 of the PIPL responds to the issue by providing that, the installment of any image capturing or personal identification equipment in a public place shall be necessary for maintaining public security, comply with the relevant regulations, and be accompanied with a prominent sign indicating the existence of such equipment. In addition, any personal image or personal identification information of an individual collected can only be used for the purpose of maintaining public security, and shall not be used for any other purpose, except with separate consent obtained from the individual.

5. Specific Rules for Handling Sensitive Personal Information

a) Definition of sensitive personal information

Sensitive personal information is a specific type of personal information and subject to stronger protection under the PIPL. Therefore, it is important for enterprises to sort out sensitive personal information from the handled personal information based on the definition under the PIPL and follow the specific rules for handling sensitive personal information.

According to Article 28 of the PIPL, sensitive personal information refers to personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric identification, religious belief, specific identity, medical and health information, financial accounts, personal whereabouts, etc., as well as any personal information of a minor under the age of 14. The PIPL also emphasizes that personal information handlers may handle sensitive personal information only when there is a specified purpose and sufficient necessity, and strict measures shall be adopted for protecting the handled sensitive personal information.

b) Special protection for minors

Compared with the second draft of the PIPL, the PIPL newly includes the personal information of a minor under the age of 14 into sensitive personal information, which implies stronger protection for a minor's personal information. Further, for handling personal information of a minor under the age of 14, personal information handlers shall obtain the consent from his or her parent or guardian according to Article 31 of the PIPL. In addition, special rules for handling such minors' personal information shall be established by relevant personal information handlers. Based on the above, enterprises should pay more attention to these special requirements, if handling certain minors' personal information.

c) Notification and consent requirement for handling sensitive personal information

In addition to the required notification contents as stated above in Item 4. b) (1), Article 30 of the PIPL provides that personal information handlers shall additionally notify the individual of the necessity of handling such sensitive personal information and the impact on the individual's rights and interests, except where the absence of such notification is allowed as provided by the PIPL.

After making the required notification, a separate consent shall be obtained from the individual for handling of his or her sensitive personal information according to Article 29 of the PIPL. Further, a written consent shall be obtained for handling sensitive personal information, if it is provided by relevant laws and regulations. The PIPL does not provide a definition for separate consent, but based on the plain meaning it seems to require that consent shall be given in particular for the involved sensitive personal information and not as part of any packaged or bundled consent for numerous types of personal information.

6. Rules for Cross-border Transfer of Personal Information

Cross-border transfer of personal information is an important and strictly regulated personal information handling activity under the PIPL. Enterprises shall pay attention to the following requirements for cross-border transfer of personal information.

a) Data localization and security assessment obligations for specific handlers

Article 40 of the PIPL stipulates that critical information infrastructure operators ("CIIOs"), or personal information handlers whose handling of personal information reaches the threshold amount prescribed by the national cyberspace department, shall store within the territory of the PRC the personal information collected or generated by them within the territory of the PRC. According to Article 9 of the *Measures for Security Assessment for Cross-border Transfer of Personal Information and Important data (a consultation draft issued on 11 April 2017, not effective yet, "2017 Draft Regulation")*, the threshold amount refers to the data involving or totally involving the personal information of over 500,000 individuals or the data volume exceeds 1,000GB.

If it is necessary to provide such personal information to an overseas recipient, a security assessment organized by the national cyberspace department shall be passed in advance. If a security assessment is not required as provided by laws, administrative regulations or the national cyberspace department, such provisions shall prevail.

b) Requirements for other handlers

For other personal information handlers, Article 38 of the PIPL provides that if it is necessary to transfer personal information to a recipient outside the territory of the PRC due to any business needs or any other needs, they shall meet one of the following conditions:

(1) Where a certification of personal information protection has been given by a professional agency in accordance with the regulations of the national cyberspace department;

(2) Where a contract in compliance with the standard contract provided by the national cyberspace department has been concluded with the overseas recipient, establishing the rights and obligations of both parties;

(3) Where any other conditions prescribed by laws, administrative regulations or the national cyberspace department is met.

According to the above stipulations, enterprises may engage professional agency for a certification or execute a standard contract with the overseas recipient in order to carry out the cross-border transfer of personal information in a compliant way. However, currently the PIPL does not clarify the definition of the so-called professional agency and the standard contract has not been published by the national cyberspace department yet, which are to be clarified in future implementation rules.

c) Notification and consent requirement for cross-border transfer of personal information

The PIPL also provides specific notification and consent requirement for cross-border transfer of personal information. Article 39 of the PIPL provides that a personal information handler who transfers the personal information to an overseas recipient shall inform the individual of the organizational or personal name and contact information of the overseas recipient, the purpose and method of such handling and the type of personal information involved, as well as the way for the individual to exercise his/her rights provided for by the PIPL against the overseas recipient. In particular, separate consent from the individual shall be obtained based on the above notification.

7. Rights of Individuals in Personal Information Handling Activities

a) Specified personal information rights of individuals

In order to provide sufficient protection for personal information, the PIPL provides the following personal information rights of individuals.

- Right to withdraw consent (Article 15 of the PIPL)
- Right to be informed (Article 44 of the PIPL)
- Right to decide (Article 44 of the PIPL)
- Right to restrict (Article 44 of the PIPL)
- Right to deny (Article 44 of the PIPL)
- Right to access (Article 45 of the PIPL)
- Right to copy (Article 45 of the PIPL)
- Right of portability (Article 45 of the PIPL)
- Right to correct (Article 46 of the PIPL)
- Right to delete (Article 47 of the PIPL)
- Right to seek for explanation form personal information handlers (Article 48 of the PIPL)
- Right to complain (Article 50 of the PIPL)
- Right regarding automated decision-making (Article 24 of the PIPL)

Among the above personal information rights, the right of portability and the right to complain are newly added or supplemented compared to the second draft of the PIPL.

- Article 45 of the PIPL incorporates the right of portability by reference to the GDPR, which provides that where individuals request to transfer their personal information to a designated personal information handler who meets the conditions prescribed by the national cybersecurity department, the personal information handler requested shall provide a way for such transfer.

- Article 50 of the PIPL clarifies that if the personal information handler denies an individual's request to exercise his/her rights, the individual may bring a lawsuit in a People's Court against the personal information handler. This provision strengthens individuals' procedural rights in order to safeguard the operation of the personal information rights as stated above.

b) Rights related to a dead person's personal information

Article 49 of the PIPL creatively provides specific protection for a dead person's personal information. In the event of death of a natural person, a close relative of the individual may exercise the right to access, copy, correct, delete and other rights to the relevant personal information of the natural person as provided for by the PIPL, unless the deceased has made other arrangement before death.

8. Obligations of Personal Information Handlers

The PIPL stipulates the following compliance obligations for personal information handlers in order to guarantee sufficient protection for personal information.

a) General obligations for personal information security

Article 51 of the PIPL provides that personal information handlers shall, based on the purpose and method of handling of personal information, the type of the personal information handled and the impact on personal rights and interests, any potential security risks, etc., take the following measures to be compliant and prevent any unauthorized access to, leakage of, tampering with, or loss of personal information:

– Developing an internal management system and operating procedures;

– Managing personal information based on classification of different types of personal information;

– Taking appropriate technical security measures such as encryption and de-identification;

– Reasonably determining the operating authorizations for handling of personal information, and conducting education and training regarding personal information security for employees on a regular basis;

– Developing and organizing the implementation of emergency plans for personal information security incidents; and

– Taking any other measure as required by laws or administrative regulations.

In addition, personal information handlers shall audit the compliance conditions of their personal information handling activities regularly pursuant to Article 54 of the PIPL, but the PIPL does not stipulate an exact period for the regular audit.

Further, Article 57 of the PIPL stipulates that a personal information handler shall immediately take remedial measures, and notify the relevant authorities performing personal information protection duties and any concerned individual, if any leakage of, tampering with, or loss of personal information that occurs or may occur. The notification shall include the following content:

– The type of personal information involved, the cause of such event, the harm that may be caused;

– Remedial measures taken by the personal information handlers and any measures that can be taken by the individual in order to mitigate the harm; and

– The contact information of the personal information handler.

If the personal information handler can take measures to effectively avoid relevant harm, the personal information handler may be allowed not to notify the individual. However, if the authorities performing personal information protection duties believe that harm may be caused to the individual, they may require the personal information handler to notify the individual.

b) Personal information protection officer

Further, according to Article 52 of the PIPL, personal information handlers whose handling of personal information reaches the threshold amount prescribed by the national cyberspace department shall appoint a personal information protection officer to be responsible for supervising personal information handling activities and the protection measures taken, etc. As we stated above under Item 6 a), the 2017 Draft Regulation seems to imply that the threshold amount refers to data involving or totally involving the personal information of over 500,000 individuals or the data volume exceeds 1,000GB. Therefore, enterprises need to check if they are required to appoint the personal information protection officer according to future stipulation of the national cyberspace department.

If a personal information protection officer is required to be appointed, the relevant personal information handlers shall disclose the contact information of their personal information protection officer, and report the name, contact information and other information of such officer to the relevant authorities performing personal information protection duties.

c) Personal information protection impact assessment

For certain types of personal information handling activities as stated below, Article 55 of the PIPL stipulates that a personal information protection impact assessment shall be conducted before the activity and a record of such personal information handling activity shall be kept.

– Handling of sensitive personal information;

– Use of personal information in automated decision-making;

– Entrusting of the handling of personal information to another party, provision of personal information to another personal information handler, or disclosure of personal information;

– Cross-border transfer of personal information to an overseas recipient; or

– Any other activity of handling of personal information of an individual that will have a material impact on personal rights and interests.

According to Article 56 of the PIPL, the personal information protection impact assessment shall include the following contents. In addition, it emphasizes that the personal information protection impact assessment and the record of relevant personal information handling activity shall be retained for at least three years.

– Whether the purpose, method or any other aspect of personal information handling are legal, fair and necessary;

– The impact on personal rights and interests and level of risk on security; and

– Whether any security protection measure taken is lawful, effective and corresponding to the level of risk.

For detailed guidance on carrying out such personal information protection impact assessment, enterprises should refer to the recommended national standard *GB/T 39335-2020 Information Security Technology – Guidance for Personal Information Protection Impact Assessment*, which took effect on 1 June 2021.

d) Additional obligations of personal information handlers who provide important internet platform services

Since the personal information handlers who provide important internet platform service control a large volume of personal information of users, Article 58 of the PIPL stipulates that the relevant personal information handlers shall fulfil some obligations in addition to the general obligations as follows:

– Establishing an independent body mainly consisting of external members to supervise their protection of personal information;

– Formulating platform rules as to clarify the standards and obligations related to personal information security to be met by product or service providers on the platform;

– Ceasing the platform services to any product or service providers on the platform in a serious violation of relevant laws and regulations;

– Publishing a social responsibility report on personal information protection on a regular basis, etc.

However, it is still unclear how to identify personal information handlers who provide important internet platform services and the implementation of specific obligations. This needs to be elaborated by implementation rules or guidelines of relevant authorities to be issued in the future.

9. Authorities Performing Personal Information Protection Duties

Article 60 of the PIPL clarifies the relevant authorities in charge of personal information protection. At the national level, the national cyberspace department shall coordinate the overall supervision and management work of personal information protection while relevant departments under the State Council shall be responsible for the supervision and management work of personal information protection within their respective scopes of duties. At the local government level, the duties for supervision and regulation of personal information protection shall be performed by the relevant authorities of local people's governments at the county level or above in accordance with relevant regulations of the State. The above stated authorities are referred to as authorities performing personal information protection duties (“Competent Authorities”).

As to the duties of the Competent Authorities, there are two important issues as follows:

a) Obligations and liabilities for application programs

Article 61 of the PIPL provides that the Competent Authorities shall organize the testing and evaluation of any application programs concerning personal information protection and disclose the results to the public. Further, any application program that illegally handles personal information will be ordered to suspend or terminate its services and be subject to other administrative penalties as stipulated under Article 66 of the PIPL (see details below in Item 10 a)). In the past, the Competent Authorities have already enforced against illegal handling of personal information through application programs based on *Methods for Identifying Unlawful Acts of Applications (Apps) to Collect and Use Personal Information* (effective as of 28 November 2019) and *Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications* (effective as of 1 May 2021). After the PIPL takes effect, the Competent Authorities will have a more solid legal basis for regulating personal information handling of application programs and may implement stricter regulation in this regard.

b) Special rules for small-sized personal information handlers

Article 62 of the PIPL provides that the national cybersecurity department and the relevant authorities shall develop special rules and standards for personal information protection regarding small-sized personal information handlers, handling of sensitive personal information, face recognition, artificial intelligence and other new technologies and new applications. Since the compliance obligations under the PIPL for personal information handlers are rather strict, it may unreasonably add operation expenses for small enterprises and have negative effects on innovation. Although the PIPL does not provide a definition of small-sized personal information handlers, it implies that there may be special rules in this regard in order to avoid imposing overwhelming compliance burdens on small enterprises.

10. Legal Liabilities for Violation

The PIPL provides severe legal liabilities for violation in order to ensure stronger protection and deter potential infringement upon personal information.

a) Administrative liabilities

Article 66 of the PIPL provides that any personal information handler in violation of the PIPL or failing to perform the relevant personal information protection obligations will be ordered to make correction, be given a warning, and be confiscated of any illegal gain by the Competent Authorities. If such a personal information handler refuses to make correction, a fine of up to RMB 1 million will be imposed and any person directly in charge and any other directly responsible persons will be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000. If the circumstances of violation are serious, the personal information handler will be ordered to make correction, be confiscated of any illegal again, and be imposed with a fine up to RMB 50 million, or 5% of last year's annual revenue by the Competent Authorities at the provincial level or above. It may also be ordered to suspend any related activity or to suspend business for rectification, or be reported to the relevant authority for revocation of the related business permit or business license. In addition, any persons directly in charge and any other directly responsible persons will be imposed with a fine of no less than RMB 100,000 but no more than RMB 1 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.

Consistent with the CSL, Article 67 of the PIPL also provides that relevant violation of the law shall be marked in the credit record in accordance with relevant laws and regulations, and shall be disclosed to the public.

b) Civil liabilities

(1) Burden of proof and calculation of damages

The *PRC Civil Code* has provided a legal basis for claiming civil liabilities against any harm caused to personal information rights and interests. An important feature of the PIPL in this regard is that it specifies that the burden of proof shall be taken by the personal information handlers. Article 69 of the PIPL provides that where any damages are caused due to infringement upon personal information rights and interests during personal information handling, the infringing personal information handler needs to prove that there was no fault on his or her part. Otherwise, the infringing personal information handler shall bear tort liabilities, such as paying damages.

Further, the PIPL stipulates the calculation methods for damages caused by personal information infringement. Such damages shall be determined based on the losses suffered by the infringed individual due to the infringement, or the gains obtained by the infringing personal information handler from the

infringement. If the aforesaid losses or gains are difficult to be ascertained, the amount of damages shall be determined based on the actual situation by the People's Court.

(2) Public interest litigation

Another important stipulation is that the PIPL establishes the public interest litigation approach for personal information infringement cases. Article 70 of the PIPL provides that a People's Procuratorate, a consumer organization as specified by laws, or an organization as determined by the national cyberspace department may legally bring a lawsuit in a People's Court against a personal information handler whose handling of personal information violates the PIPL and infringes the rights and interests of a large number of individuals. One day after the publication of the PIPL, the Supreme People's Procuratorate issued the *Notice on Implementation of the PIPL to Promote Public Interest Litigation on Personal Information Protection* on 21 August 2021, which seems to imply that public interest litigation for personal information infringement cases will be in the focus of People's Procuratorate in the future.

(3) Criminal liabilities

Article 71 of the PIPL stipulates that any violation of the law that constitutes a violation of public security administration shall be subject to penalties under public security administration rules. If such violation constitutes a criminal offense, the relevant personal information handler shall be investigated for criminal liabilities in accordance with the law.

11. Conclusion

As a fundamental legislation regarding personal information regulation and protection, the PIPL stipulates detailed rules for handling personal information and responds to practical issues regarding personal information, such as automated decision-making, biometric identification, handling of personal information by application programs. Enterprises shall review their current practice based on the compliance obligations stipulated by the PIPL and make internal alignment before the PIPL takes effect. Meanwhile, we expect to see relevant implementing rules and guidelines promulgated by the relevant authorities in the near future in order to clarify administrative procedures for fulfilling the relevant obligations in practice.

In case you have questions or for further information, please contact the authors of this newsletter:

Panpan Tang
Associate
CMS, China

T +86 21 6289 6363
E panpan.tang@cmslegal.cn

Spring Zhu
Junior Associate
CMS, China

T +86 21 6289 6363
E spring.zhu@cmslegal.cn

About CMS, China
关于 CMS, 中国

CMS is one of the top 10 global law firms. With more than 4,800 professional legal and tax advisors in over 70 offices in more than 40 countries, we advise clients on both global and local matters and provide pragmatic and commercial advice.

CMS, China has been advising clients on doing business in China for several decades. As one of the top international law firms in China, we are able to support international companies and Chinese enterprises on all their legal needs through our full service offering. We advise in the areas of M&A, corporate restructuring, FDI, distribution and commercial, competition, compliance, employment, banking and finance, insurance, real estate and construction, technology licenses, IP registration and enforcement, dispute resolution as well as tax and customs.

Our team of legal experts are from China, Germany and the UK, and have an in - depth knowledge and understanding in many industrial sectors such as automotive, manufacturing, machinery and equipment, life sciences and healthcare, energy, banking & finance and TMC. We focus on serving the needs of our clients and on providing them with solution driven and business-oriented advice.

作为全球最大的法律与税务服务机构之一，CMS 通过旗下遍布于 40 多个国家超过 70 个办公室的 5,000 多名律师，提供覆盖全球及本土化的商业可行性解决方案。

如今，CMS 在中国服务客户已有数十年的历史。作为中国最大的外资律所代表处之一，CMS, 中国专注于并购、公司重组、外商直接投资、分销和商法、竞争法、合规、劳动法、银行 和金融、保险、房地产和建筑、技术许可、知识 产权注册与执行、争议解决及税务和海关等各个领域， 为国际与中国公司提供全方位的法律咨询服务。

我们的顾问团队由来自中国、德国和英国的专家组成，对汽车、制造、机械设备、生命科学和医疗保健、能源、银行金融以及技术、传媒与通讯等行业领域有着全面深入的了解。我们注重为客户提供实际有效的咨询和解决方案， 以帮助客户达到既定商业目标。

3108 Plaza 66, Tower 2, 1266 Nanjing Road West, Shanghai 200040 P.R.China
上海市南京西路 1266 号恒隆广场 2 期 3108 室

Phone/ 电话: + 86 21 6289 6363

Fax/ 传真: + 86 21 6289 0731

Web/ 网址: https://cms.law/ en/ chn/

Email/ 电邮: info@cmslegal.cn

Welcome to follow our WeChat account where you will find the updated legal insights and news.

欢迎扫码关注我们的微信公众号，在这里您可以获取最新的法律资讯和新闻。