中倫律師事務所
ZHONG LUN LAW FIRM
北京市朝阳区金和东路 20 号院正大中心 3 号楼南塔 23-31 层，邮编：100020
23-31/F, South Tower of CP Center, 20 Jin He East Avenue, Chaoyang District, Beijing 100020, P. R. China
电话/Tel：+86 10 5957 2288　传真/Fax：+86 10 6568 1022/1838
网址：www.zhonglun.com

A New Era of Data Compliance in China: Highlights of the Personal Information Protection Law

John Jiang, Rachel Li, Jason Jia, Peter Zhong, Megan Li[1]

On August 20, 2021, the National People's Congress of China passed the *Personal Information Protection Law of the People's Republic of China* (the "**PIPL**"), which will come into force on November 1, 2021 and serve as the foundation of China's personal information protection legal system. With seventy-four articles, the PIPL comprehensively stipulates the protection obligations and responsibilities of personal information processors, and the rules for and boundaries of various Processor's information processing activities.

For the first time in China, the PIPL lays out a comprehensive and strict set of rules around personal information processing activities and established a rigorous regulation system over personal information protection, which creates significant regulatory requirements for multinationals with operations in China or sells to Chinese consumers. While the approach of PIPL overlaps with the GDPR to some extent, there are also significant deviations; for instance, unlike the GDPR, the PIPL broadly categorizes persons which process personal information in any stage by any means as "personal information processors" (the "**Processors**").

In this article, we will summarize several highlights of the PIPL and explore their implications.

Highlight 1: Classification of Individuals' Various Rights Over Personal Information and Adding the New Right to Data Portability

The PIPL devotes an entire chapter (*Chapter IV - Rights of Individuals in Activities of Processing of Personal Information*) to individuals' various rights to their personal information in three aspects, collection of their personal information, its maintenance, and gaining access to it, as illustrated in the table below.

Stages	Rights and Interests	Specific Requirements
Collection	Right to be Informed	Individuals should be informed of the collection and processing of his/her personal information in a conspicuous way, in clear and easy-to-understand language, and in a truthful, accurate and complete manner
	Right to	Individuals have the right to refuse the making of decisions by the

	Refuse Automated Decision Making	personal information processor solely by means of automated decision-making.
	Right to Request Explanation	Individuals have the right to require personal information processors to explain their rules of processing of personal information.
Maintenance	Right to Request Correction and Supplement	Individuals have the right to request personal information processors to correct or complete their personal information.
	Right to Delete	The Processors should delete the personal information of the relevant individual when any of the following circumstances happens: • the purpose of processing has been achieved or is unable to be achieved, or the personal information is no longer necessary for achieving the purpose of processing; • the personal information processor ceases the provision of the product or service involved, or the retention period has expired; • consent is withdrawn by the individual • the processing of personal information by the personal information processor is in violation of any law, administrative regulations or agreement; • there is any other circumstance as provided by law or administrative regulations requiring the Processor to delete the personal information.
Access	Right to Access and Copy	Individuals have the right to access or make copies of their personal information.
	Succession Right	In the event of death of an individual, a close relative of the individual may exercise the rights to access, make copies of, have corrected or deleted and/or other rights to the relevant personal information of the individual as stipulated by law, unless the deceased has arranged otherwise before death.
	Right to Data Portability	Processors shall meet individuals' request to transfer their personal information to another personal information processor designated by him/her.

Notably, right to data portability (i.e. the last right listed in the table above) has been newly added into the PIPL in its final review round during the legislation process. This right to data portability under the PIPL is a bit different from that provided under the GDPR, which has following key

features: (1) the data subject shall have the right to receive the personal data from controller and processor; (2) the data format is structured, commonly used and machine-readable; and (3) the data subject have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. Th PIPL data portability right is aimed to break down the current non-interoperability and non-transferability between different APPs to avoid "isolated data islands". It remains to be seen how this can be effectively implemented for consumer facing enterprises.

Highlight 2: "Informing-Consent" Mechanism of Personal Information Processing Activities Stream and Special Rules for Sensitive Personal Information.

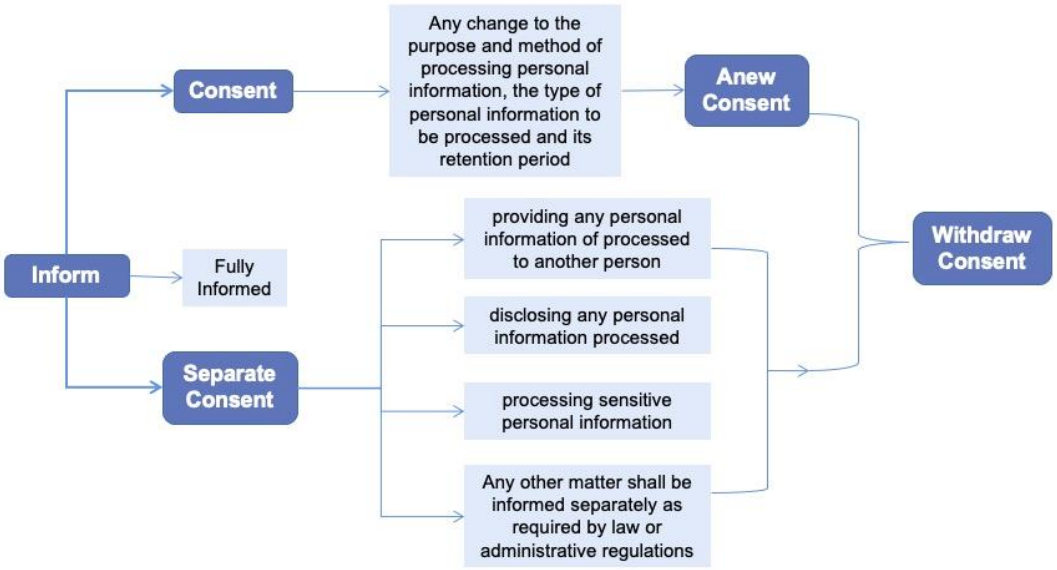
Based on the lifecycle of personal information processing, PIPL clearly stipulates that the processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information. Prior to conducting any processing activities of any personal information, the Processor shall inform the individual of how it would process his/her personal information in a conspicuous way, in clear and easy-to-understand language, and in a truthful, accurate and complete manner; and the Processor should obtain the individual's consent before processing his/her personal information. Further, the PIPL establishes several special consent requirements as follows:

- **Separate Consent Requirement**: the Processor shall obtain separate consent from the relevant individuals when the Processor provides others with his/her personal information of biometric recognition, medical and health, financial account, personal whereabouts and other information as stipulated by law.
- **Re-Consent Requirement**: the Processor shall obtain consent again from the individual in the event of any change in the purpose or method of processing his/her personal information or in the event of any change in the type of personal information to be processed. Where a Processor needs to transfer personal information of any individual due to a merger, division, dissolution, bankruptcy or any other reason, or the personal information aforementioned provided to others changed, it shall also obtain consent from the individuals once again.
- **Special Consent Requirement over Sensitive Personal Information**. The PIPL establishes a clearer definition of sensitive personal information by giving a general description and listing specific examples. The Processor has to obtain specific consent from individuals for sensitive personal information, with the prerequisite that the individuals have been informed of the "specific purpose and sufficient necessity" of the processing, and the Processor has to "take strict protection measures" to protect sensitive personal information. Besides, personal information of a minor under the age of 14 is included in the scope of sensitive personal information as well, and the PIPL requires the Processors to establish special processing rules for such minor's information, reflecting the special concern of the PIPL for the protection of personal information of minors.

  The table below illustrates key take-aways relating to sensitive personal information:

Concept	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 recognition, religious belief, specific identity, medical and health, financial account, personal whereabouts and other information of a natural person, as well as any personal information of a minor under the age of 14.
Principle	Processors may process sensitive personal information only when there is a specified purpose and sufficient necessity and there are strict measures adopted for its protection.
Stricter Informed Consent Mechanism	• Inform the individuals when processing sensitive personal information; • Inform the individual of the necessity of processing such sensitive personal information and the impact on the individual's rights and interests; • Obtain specific consent from the individual.

In response to the widespread practice of "not allowing individuals to use the APP unless the consent is given" and to suppress the non-essential bundling of access to individual's personal information to other activities, the PIPL clearly stipulates that Processors "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".



Although the principle of informed consent is the primary legal basis for lawful processing of personal information, there are also some circumstances under which the consent is not necessary, depending on the complexity and circumstances of the personal information processing activity as provided in Article 13 of the PIPL (Please see the sheet below). Compared to the Second Review Draft of PIPL, the PIPL provides that entities may process personal information without first obtaining consent where necessary for human resource management under an employment policy legally established or a collective contract legally concluded. Besides, personal information which

has been disclosed to the public can be reasonably processed without consent, unless such processing is expressly refused by the individual. This provision leaves some room for enterprises to process publicly disclosed data.

Below is a table illustrating the stipulated circumstances where Processors can process personal information without obtaining the relevant individuals' consent:

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 an employment policy legally established or a collective contract legally concluded;
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 processed within a reasonable scope to carry out any news reporting, supervision by public opinions or any other activity for public interest purposes;
5	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;
6	Any other circumstance as provided by law or administrative regulations.

Furthermore, even the "Informing-Consent" requirement is met on the face, the Processors should also comply with the following substantive principles of personal information processing, which is stipulated in the opening paragraph of the PIPL: (1) that the processing activities shall be conducted in a way that has the least impact on the rights and interests of individuals, (2) that the collection shall be limited to the minimum scope necessary for achieving the purpose of processing, and (3) that the retention period shall be the minimum period necessary for achieving the purpose of processing. Therefore, if the actual processing activities fail to abide by the substantive principles, the Processors would be exposed to compliance risk even if it has obtained consent from the individuals for personal information processing.

Highlight 3: Establishment of Rules for the Cross-border Provision of Personal Information

In chapter III (*Rules of Cross-border Provision of Personal Information*), the PIPL establishes a systemic approach to the regulation of the cross-border transfer of personal information and the related review mechanism, the highlights of which are summarized in the table below.

Circumstances	Key points	Specific Requirements
General Rules for Provision of Personal Information to a Recipient	One out of the Four Legitimate Circumstances	• Passing the security assessment organized by the national cyberspace authority; • Receiving a certification of personal information protection given by a professional institution in accordance with the regulations of the national cyberspace authority;

Outside the Territory of China		• Concluding a contract in compliance with the standard contract provided by the national cyberspace authority with the overseas recipient; or • Meeting any other condition prescribed by law, administrative regulations or the national cyberspace authority.
	Informed and Separate Consent	• Informing the individual of the related information of the overseas recipient and for the individual to exercise his/her rights; • Obtaining separate consent.
	Safeguarding Obligation	• Processors shall take any necessary measure to ensure that the activities of processing of the personal information provided by them carried out by overseas recipients meet the standards of personal information protection provided in this Law.
Special Requirements for Special Processors	Subject Scope	• Critical information infrastructure operators; • Processors whose processing of personal information reaches the threshold amount prescribed by the national cyberspace authority. [2]
	Storage Within the Territory	• Shall store the personal information collected or generated in China within the territory of China.
	Cross-border Provision	• Shall pass a security assessment organized by the national cyberspace authority; • Other circumstances under which security assessment is not required.
Foreign Judicial or Law Enforcement Agencies.	Subject and Behavior	• foreign judicial or law enforcement agencies; • provision of any personal information stored within the territory of China.
	Cross-border Provision	• Without the approval of competent authorities, Processors shall not provide any personal information stored within the PRC territory to a foreign judicial or law enforcement agencies.
The List of restricted or prohibited recipients	Subject and Behavior	• Any organization or individual outside China engaged in any activity of processing of personal information that infringes on the personal information rights and interests of any citizen of China; • Any organization or individual outside China engaged in any activity that endangers the national security or public interests of China.
	List	• Such foreign entities shall be included in a list of restricted or prohibited recipients for the provision of personal information and be publicly announced. • Such foreign entities shall be restricted or prohibited from

		being recipients for the provision of personal information.
The Reciprocity Principle	Subject and Behavior	• Any country or region that takes any discriminatory prohibition, restriction, or any other such measure against China in respect of personal information protection.
	Measures	• China may take reciprocal measures depending on the actual situation.

It is worth mentioning that in the First Review Draft of the PIPL, the Processor is only required to enter into a contract for the cross-border transfer of personal information, without specifying requirement on terms of such contract; however, the official PIPL explicitly requires that the contract concerning cross-border transfer of personal information shall be "in compliance with the standard contract provided by the national cyberspace authority", indicating that the national cyberspace authority will publish standard data processing contract for cross-border transfer of personal information. This change reflects the trend towards stricter regulation of cross-border personal information transfer.

Highlight 4: Establishment of Rules for the Application of Personal Information in Automated Decision-making

Automated decision-making activities are widely used, such as the collection of personally identifiable information, consumer consumption information. For example, the data-based algorithm for user profile has been widely used in commercial advertising and product recommendation. The PIPL establishes the rules for using personal information for automated decision-making[3] such as user profiling and algorithm recommendation, especially guarding against the excessive collection of personal information and "big-data based discrimination" by APPs, as summarized in the table below:

Principles	• Processors shall procure the transparency of the decision-making and the fairness and justice of the handling result of automated decision making； • Processors shall not apply discriminatory treatment to consumers in terms of price and service terms by means of automated decision-making.	
Requirements	Personal Information Protection Mechanism under Different Circumstances	Push-based Information Delivery or Commercial Sales：Processors shall simultaneously provide the option to not target an individual's characteristics or provide the individual with a convenient method to decline.
		Material Impact on Individual's Rights and Interests: an individual shall have the right to demand the Processor to provide an explanation, as well as the right to refuse the making of decisions by Processor solely by means of automated decision-making.
	Personal Information Protection Impact	Processors shall conduct a personal information protection impact assessment in advance, and record the processing situation in the event of using personal information to conduct automated decision-making.

	Assessment and Record	

Through the special provisions concerning automated decision-making, the PIPL addresses increasing public concern for the protection of personal information and consumer rights and interests on the Internet, and reflects the government's intention to form a strong regulatory system together with laws and regulations in other sectors for synergistic enforcement on the issue of "big-data based discrimination".

Highlight 5: Aggravated Sanction on Infringement of Personal Information

For anyone processing personal information in violation of the PIPL or failing to perform any obligation of personal information protection, the PIPL prescribes penalties and other liabilities with aggravated sanctions, which include:

(1) any application program that illegally processes personal information will be ordered to suspend or terminate its services;

(2) if the illegal activity is of a grave nature, 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;

(3) the violator 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

(4) 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.

Compared to the prior drafts of the PIPL, the official draft has added a new penalty for executives to be banned from personal information processing business, forcing relevant personnel of the enterprise to fulfill their obligations and responsibilities under the PIPL. Besides, as for Processors who jointly process personal information, the PIPL states that all Processors 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.

The current enforcement activities clearly show the trend towards tighter supervision and regulation. In practice, blocking and removing law-breaking APPs from APP stores and normal operating have been the measures most in use for China's cyberspace regulators to punish the violators and require them to carry out rectification. In 2021 alone, the Ministry of Industry and Information Technology of PRC has so far announced the lists of APPs infringing on users' personal interest and rights for eight times. Another example is that in July 2021, the China's Cybersecurity Review Office announced that it had initiated network security review procedures against four mobile applications operated by Didi Chuxing ("Didi"), then Didi was removed from APP stores and halted new users

thereafter.

Highlight 6: Creating Special Obligations for Important Internet Platforms and Building Systematic Obligations for Processors

For keeping up with the global boom in digital services and the development of digital market rules, the PIPL creates special obligations for a particular type of processor, namely important internet platform. This is similar to the draft *Digital Services Act* of EU, which requires high transparency and strict accountability mechanisms for online platforms, especially for very large online platforms which provide services to a number of users equal to or higher than 45 million, stricter obligations to risk management, independent audit and public reports shall be performed. Under the PIPL, three features shall be considered when defining important internet platform shown in the table below.

The PIPL imposes four special obligations on important internet platform processors to protect personal information: (1) establishing a personal information protection compliance policy and external independent supervision body, (2) developing platform rules in accordance with the principles of openness, fairness, and impartiality, (3) ceasing the provision of any service to any product or service provider operating on their platform who commits a serious violation of the PIPL, and (4) publishing a social responsibility report on personal information protection.

After establishing the special compliance obligations for the important internet platform, a wave of enforcement is expected for the protection of personal information on important online platforms. It is worth mentioning that Article 62 of the PIPL explicitly provides that the national cyberspace authority shall develop special rules and standards for personal information protection regarding small personal information processors, leaving room for legislation for such processors. In the next stage, the national cyberspace authority may design special rules for such processors in terms of lighter requirements and exemptions from liability, which will reinforce the flexibility and enforceability of relevant rules.

Special Obligations of Important Internet Platform	
Definition of Important Internet Platform	Providing important internet platform service.
	Having a large user base.
	Operating a complex type of business.
Special Obligations and Responsibilities	(1) Establishing a sound personal information protection compliance policy and system in compliance with the laws and regulations and establishing an independent body that is mainly composed of external members to supervise their protection of personal information.
	(2) Developing platform rules in accordance with the principles of openness, fairness, and impartiality, specifying the standards for processing of personal information and the obligations of personal information protection to be met by product or service providers operating on their platform.

	(3) Ceasing the provision of any service to any product or service provider operating on their platform who commits a serious violation of any law or administrative regulation in the processing of personal information.
	(4) Publishing social responsibility report on personal information protection on a regular basis and accepting supervision from the public.

Conclusion

In recent years, both lawmakers and regulators have paid great attention to individual's personal information protection, raising great challenge to compliance of market players. The PIPL, together with the *Data Security Law* and the *Cybersecurity Law*, constitute the three fundamental laws in the field of network security and data compliance in China. These three laws and respective supporting regulations, target to protect the orderly development of China's cyberspace security from different perspectives and dimensions. Therefore, it is crucial for enterprises involved in data and personal information processing activities to quickly establish a compliance system to address the rapidly-growing and challenging requirements provided by the aforesaid three laws.

[1] Rachel Li is an equity partner, John Jiang and Jason Jia are senior counsels at Zhong Lun, specializing in data compliance, antitrust and M&A. Gengjun Li and Joyce Chen also contributed to this paper.

[2] Under Article 6 of the Revision Draft of *Revision Draft of Measures for Cybersecurity Review (Exposure Draft)*, network operators who possess the personal information of more than 1 million users and list abroad shall declare cybersecurity review to the Cybersecurity Review Office, which may clarify the standards for the "number prescribed by the national cyberspace authority".

[3] Under the Article 73 of PIPL, "Automated decision-making" refers to an activity of conducting any analysis or assessment of the behavior and habits, interests and hobbies, financial, health or credit status or other information of an individual, as well as any decision-making automatically through a computer program.