LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice September 8, 2021 | Number 2894

China Introduces First Comprehensive Legislation on Personal Information Protection

The Personal Information Protection Law, or PIPL, imposes stringent obligations of a similar standard to the GDPR and will take effect on November 1, 2021.

Key Points:

- **Extraterritorial effect:** PIPL applies to those who process personal information about Chinese individuals *inside* China as well as those who process personal information about Chinese individuals *outside* China.
- **Legal basis:** PIPL expands the legal bases for processing personal information to seven, including where it is necessary for the performance of a contract with the individual.
- **Data transfer restrictions and localization requirements:** Critical information infrastructure operators (CIIOs) and those who exceed the threshold of personal information processed set by the Cyberspace Administration of China (CAC) must store personal information in China unless they pass a CAC security assessment. PIPL also imposes more stringent requirements on cross-border data transfers, e.g., consent of the individual is always required.
- **Fines:** Those who violate PIPL may face fines of up to 5% of annual revenue of the previous year or CNY50 million.

On August 20, 2021, the Standing Committee of the National People's Congress adopted the Personal Information Protection Law of the People's Republic of China (PIPL), the first legislation dedicated to protecting personal information in China. PIPL will take effect on November 1, 2021.

PIPL previously underwent two revisions: the First Draft in October 2020 and the Second Draft[1] in April 2021. Prior to PIPL, personal information in China was protected largely by the Network Security Law (which took effect in June 2017), the Civil Code (which took effect in January 2021), various provisions in other laws, and the Data Security Law, which was adopted in June 2021 and took effect on September 1, 2021. Collectively, these legislative sources will provide a comprehensive legal framework for protecting personal information in China.

Overview

PIPL aims to improve and advance the existing legal framework on the protection of personal information. For example, PIPL will:

- Expand the **legal bases** for processing personal information
- Include provisions on **automated decision-making** and collecting images and identification information in public places in response to emerging social issues
- Stipulate rules and restrictions on **cross-border transfers of personal information**
- Clarify the **personal information rights of individuals** and the obligations of personal information processors

Jurisdictional Scope

PIPL has extraterritorial effect and applies to processing activities that take place both inside and outside the territory of China.

Processing activities inside China: The first paragraph of Article 3 of PIPL states that PIPL applies to the processing of personal information of natural persons *inside* China.

Processing activities outside China: The second paragraph of Article 3 of PIPL states that PIPL applies to the processing of personal information carried out *outside* China, where the purpose is (i) to provide products or services to natural persons in China; or (ii) to analyze or assess the activities of natural persons in China.

Key Concepts

Definition of "personal information": According to Article 4[2] of PIPL, personal information is "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons." The inclusion of the terms "related," "identified," and "identifiable" suggests that Chinese authorities likely will take a broad approach to interpreting what constitutes personal information in practice. Article 4 also clarifies that anonymized data shall not be considered personal information.

Definition of "personal information processing": Similar to the Data Security Law, "personal information processing" is defined in Article 4 of PIPL as including "the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information." Notably, "deletion" was not included in the Second Draft but is included in the final version.

Definition of "personal information processors": Personal information processors are subject to most of the requirements in PIPL and are defined in Article 73 as "organizations and individuals that can independently determine processing purposes, and processing methods."

Principles and Legal Basis for Personal Information Processing

Principles for Personal Information Processing

Articles 5 to 9 of PIPL set out the principles for personal information processing. These principles include legality, propriety, and sincerity, which are also noted in the Network Security Law and the Civil Code.

The principle of necessity is explained in Article 6 of PIPL,[3] which stipulates that personal information processing shall "have a clear and reasonable purpose," "directly related to the processing purpose," and "limited to the smallest scope for realizing the processing purpose." This important principle underpins many of the requirements in PIPL and is evident in other rules and regulations in the context of personal information processing prior to the publication of PIPL. For example, in March 2021, the CAC, the State Administration for Market Regulation (SAMR), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Public Security issued the Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications (Rules on the Scope of Necessary Personal Information of Apps), which stipulate the scope of "necessary personal information." The Rules on the Scope of Necessary Personal Information of Apps emphasize that users will not be rejected from using basic functional mobile internet app services if they fail to provide unnecessary personal information.

In addition, the Personal Information Security Specification (a national standard developed by National Information Security Standardization Technical Committee, which took effect on October 1, 2020) provides that "directly related to the processing purpose" means the personal information which must be provided, otherwise the products or services cannot function.

Articles 7 to 9 of PIPL set out other personal information principles, including openness and transparency, quality of personal information, and responsibility for processing personal information.

Legal Basis for Personal Information Processing

Instead of relying only on "notification and consent" as established in the Network Security Law, PIPL requires personal information to be processed under one of the legal bases set out in Article 13.

What are the most relevant legal bases for organizations processing personal information?

Necessity for contracts or human resources (HR) management

The final version of PIPL includes a legal basis for processing that is "necessary to conduct human resources management under the labor rules formulated and the collective contracts entered into in accordance with laws." This legal basis was not included in earlier drafts, which only provided for processing that is "necessary to conclude or fulfill a contract in which the individual is a contracting party," suggesting that the legislator expects this (HR management) to be the future legal basis for processing employee personal information.

Moreover, the necessity for HR management in this provision is limited to that generated from "lawfully formulated labor rules and structures and lawfully concluded collective contracts." Such a provision may motivate companies to structure internal labor rules in accordance with relevant laws and regulations (e.g., the democratic procedures in Article 4 of the Labor Contract Law).

Personal information already disclosed

Another legal basis is the processing of "personal information already disclosed by persons themselves or otherwise lawfully disclosed." This provision is refined by Article 27, which states that a person can "clearly refuse" the processing on their personal information already disclosed and that consent from such person is still required if the processing of their personal information has "a major influence on individual rights and interests." Such provisions are generally consistent with Article 1036 of the Civil Code.[4]

The First Draft and the Second Draft set many restrictions on processing disclosed personal information, including that the information must not be used for purposes beyond those for which it was disclosed (otherwise consent is required). The final version does not include those detailed restrictions, but does

specify that disclosed personal information shall be processed "within a reasonable scope." Some practitioners suggest that a "reasonable scope" requires consideration of the purpose of the disclosure, the person's expectation of privacy, and the effect of the use of the disclosed personal information on the person's rights and interests.[5] However, practitioners should look to future enforcement and judicial cases for clarity on the definition of "reasonable scope".

Forms and criteria of consent

Consent forms another of PIPL's legal bases which personal information processors may rely on when processing personal information. Articles 14 and 15 clarify that consent is only valid if individuals voluntarily and explicitly provide such consent and with full knowledge of the details of the personal information processing. Individuals also have a right to withdraw consent, and personal information processors must provide individuals with a convenient means of withdrawing consent.

Article 14 also introduces the concept of "separate consent," specifically "[w]here laws or administrative regulations provide that a separate consent or written consent is required in order to process personal information, those provisions shall prevail." This concept is also used in other articles of PIPL, including those on publicly collected information, sensitive personal information, and cross-border transfer of personal information. There is currently no definition or specific procedure specified for obtaining separate consent, but a separate pop-up consent window likely will suffice in practice.

Specific Rules on Personal Information Processing

Automated Decision-Making

Automated decision-making is defined in Article 73 of PIPL as "the use of computer programs to automatically analyze or assess individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status, etc., and engage in decision-making activities."

Article 24 imposes the following restrictions on automated decision-making:

Prohibition on Differential Pricing on Existing Users

The first provision of Article 24 stipulates that automated decision-making shall guarantee the transparency of the process and the fairness and justice of the result, and personal information processors may not engage in unreasonable differential treatment of individuals in trading conditions such as trade price. This provision targets the trend of "differential pricing on existing users," which refers to using big data analytics to differentiate and apply different pricing strategies to user groups, such as those who are not price sensitive, which often results in higher prices for existing users than for new users

Before the adoption of PIPL, the SAMR published the draft Regulations on Administrative Penalties for Price Violations (July 2021) and draft Regulations Prohibiting Unfair Competition on the Internet (August 2021), which also contain provisions on differential pricing from the perspective of price discrimination and unfair competition. Currently, enforcement of the regulations and judicial cases relating to differential pricing based on big-data analytics are rare,[6] however, the PIPL is expected to change that.

Some practitioners point out that Article 24 does not intend to prohibit all kinds of differential pricing (e.g., discounts for new users), but rather emphasizes that such conduct should not lead to unfair results.[7] However, how the legislation is applied in practice will determine where the line is drawn on differential pricing.

Targeted Advertising

The second provision of Article 24 stipulates that information push delivery, or commercial sales to individuals through automated decision-making methods, shall simultaneously provide the option to avoid targeting an individual's characteristics or a convenient method for the individual to refuse or opt out of targeting. This provision focuses on what is commonly known as targeted advertising, with an emphasis on users' right to opt out (i.e., turn off ads) of targeting for marketing purposes or targeting based on personal characteristics.

Targeted advertising is currently an important issue in China. Indeed, the practice of providing false turn-off buttons in targeted information push delivery was recently included in the MIIT's Special Rectification Campaign of the Internet Industry.[8] Under the PIPL, companies using personal information for display and push delivery of targeted information or advertising should pay attention to the user's right to know (e.g., distinguishing between targeted and non-targeted contents) and the user's right to choose (ensuring that users can refuse targeted content).

Image Collection or Personal Identity Recognition in Public Venues

Article 16 of PIPL stipulates that image collection or personal identity recognition in public venues can only be used for safeguarding public security, except if individuals' separate consent is obtained. This provision responds to the social concern about some companies collecting user image information in public places, and also supports the recent efforts of the Ministry of Public Security, SAMR, and MIIT to combat underground industries such as camera peeping (e.g., use of camera technology to conduct crimes such as upskirting).[9] PIPL suggests that companies examine the image collection equipment in operation sites, factories, and similar facilities, to avoid non-compliance under this provision.

Sensitive Personal Information

According to Article 28 of PIPL, sensitive personal information refers to personal information that, once disclosed or illegally used, may easily cause grave harm to the dignity, personal, or property security of natural persons, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14 (which is newly added in the final version, but not included in the First Draft or the Second Draft). The definition and examples in Article 28 are generally consistent with those in the Personal Information Security Specification.

Article 29 stipulates that, to process sensitive personal information, the individual's separate consent must be obtained. It is unclear whether the separate consent in this provision is the only prerequisite for processing sensitive personal information, or whether the other legal basis in Article 13 can also be applied. Some commentators believe that since the scope of sensitive personal information in PIPL is relatively broad, including healthcare and financial accounts, the other legal bases for processing personal information contained in Article 13 shall still be applicable, but only the legal basis of "consent" must be in the form of "separate consent."[10]

Notably, certain categories of sensitive personal information, such as medical health data, financial accounts, are specifically regulated in other laws and regulations.[11] Therefore, companies should classify different types of personal information accordingly.

Cross-Border Transfer of Personal Information

PIPL Requirements

Prior to PIPL, requirements on the cross-border transfer of personal information were set out in the Network Security Law, but only in relation to CIIOs. None of the draft regulations regarding the cross-border transfer of personal information prior to PIPL have come into effect.

Articles 38 to 40 of PIPL provide for the requirements below on cross-border transfer of personal information for different personal information processors. CIIOs and personal information processors who reach the processing quantity thresholds prescribed by relevant authorities must store personal information collected and produced in China domestically unless they satisfy the cross-border transfer of personal information requirements set out below.

<table>
<tr><th>Personal information processor</th><th>General requirements</th><th>Specific requirements</th></tr>
<tr><td>• CIIOs
• Personal information processors who reach the processing quantity thresholds prescribed by relevant authorities</td><td rowspan="2">• Adopt necessary measures to ensure the foreign receiving parties' personal information processing activities reach the standard provided in PIPL (this requirement is newly added in the final version, but not included in the First Draft or the Second Draft);
• Notify the individuals of the foreign receiving party's contact information, processing purpose and processing methods, categories of personal information, and procedures to exercise their personal information rights over the foreign receiving party;
• Obtain individual's separate consent; and
• Conduct personal information protection impact assessments in advance.</td><td>• Pass a security assessment organized by State cyberspace authorities.</td></tr>
<tr><td>• All other personal information processors</td><td>• Conclude a contract with the foreign receiving party in accordance with a standard contract formulated by the CAC;
• Undergo personal information protection certification conducted by specialized bodies according to the requirements of the CAC; or
• Comply with other conditions provided by laws or administrative regulations prescribed by the CAC.</td></tr>
</table>

On July 30, 2021, the State Council promulgated Security Protection Regulations on the Critical Information Infrastructure (the Regulations), which took effect on September 1, 2021. The Regulations contain detailed provisions on the identification of and responsibilities of CIIOs, but do not address cross-border data transfer. The standard cross-border transfer contract and the procedures for "personal information protection certification conducted by specialized bodies" have not been published either. Detailed regulations likely will be published in the future to implement such requirements of PIPL.

PIPL Restrictions on Data Requests from Foreign Law Enforcement Authorities

According to Article 41 of PIPL, Chinese competent authorities are responsible for processing foreign judicial or law enforcement authorities' requests regarding the provision of personal information. Article 41 states that personal information processors may not provide personal information stored within the territory of China to foreign judicial or law enforcement agencies without the approval of Chinese competent authorities. This provision is similar to the restrictions on cross-border transfers of data in other Chinese laws, such as Article 177 of the amended Securities Law. It is also in accordance with the approach taken by Chinese authorities on the provision of data (not limited to personal information) to foreign judicial or law enforcement agencies.

Individuals' Rights in Personal Information Processing

Articles 44 to 48 of PIPL set out nine rights that individuals have in respect of their personal information, including the right to:

- **Know** and **decide** on the processing of their personal information
- **Restrict** or **refuse** the processing of their personal information
- **Access** and **copy** their personal information from personal information processors
- **Obtain and reuse** their personal information for their own purposes across services (i.e., data portability)
- **Correct** and **delete** personal information

Most of these rights have been covered in the Personal Information Security Specification or previous draft regulations, such as the Interim Regulations on the Administration of Personal Information Protection for Mobile Internet Applications (Interim Regulations on Mobile Internet Apps).

The final version of PIPL incorporates the "right to data portability." According to Article 45, personal information processors shall provide a channel to transfer personal information to another processor designated by the individuals as requested. This right to data portability was not included in the First Draft or the Second Draft. Notably, Article 45 doesn't specify the prerequisites or procedures for personal information processors to comply with the right to data portability.

The most commonly understood "right to data portability" is the one under the General Data Protection Regulation (GDPR) of the European Union. According to the GDPR, personal information transferrable under the right to data portability shall:

- Be obtained through consent or contract, and processed in an automated manner
- Not include the data created by the processors, such as user portrait

- Be structured, readable by machines, and in a commonly accepted format

It is unclear whether Chinese law enforcement and judicial authorities will follow the above GDPR principles in respect of the right to data portability under PIPL.

Personal Information Processor's Obligations

Articles 51 to 56 of PIPL stipulate the obligations of personal information processors in terms of staffing and organization, administrative, and security measures, as shown in the below table.

Staffing and organization	• **DPO:** Appoint personal information protection officers (if the amount of personal information processed reaches a certain threshold) • **Local representative:** Establish a dedicated entity or appoint a local representative within China to be responsible for personal information issues (for personal information processors outside China)
Internal administrative measures	• **Internal systems:** Formulate internal management systems and operating rules on personal information processing • **Audits:** Administer regular personal information compliance auditing • **PIAs:** Conduct personal information protection impact assessments
Security measures	• **Information classification:** Classify and implement categorized management on personal information • **Technical measures:** Adopt technical security measures to protect personal information such as encryption and de-identification. • **Training:** Access control and regular security education and training for employees • **Incident response:** Formulate and implement personal information security incident response plans

Provisions for Special Personal Information Processors

Important internet platforms

Article 58 of PIPL sets out the following obligations on "personal information processors providing important Internet platform services, who have a very large number of users, and whose business models are complex":

- Establish personal information protection compliance structures and systems and an independent body composed mainly of external members to supervise personal information protection circumstances

- Clarify the standards for product/service providers' processing of personal information within the platform and their personal information protection duties

- Stop providing services to product/service providers within the platform that seriously violate laws or regulations in processing personal information

- Regularly release personal information protection social responsibility reports, and accept social supervision

Notably, not all internet platforms must comply with the obligations under Article 58. Only those "important Internet platforms who have a very large number of users and whose business models are complex" are subject to the above obligations, although the criteria is not explained in details in PIPL.

Small-scale personal information processors

In both the GDPR and the California Consumer Privacy Act (CCPA), there are exemptions for small businesses to prevent excessive compliance burdens from curbing innovation. Article 62 of PIPL follows this trend by requiring relevant authorities to establish specific personal information protection rules and standards for small-scale processors. The provision does not give a specific definition of small-scale personal information processors. With reference to the GDPR and the CCPA, the criteria may include turnover, volume of personal information processed, and the percentage of revenue from the sale of personal information.

Persons entrusted to process personal information

Article 59 of PIPL stipulates that persons entrusted to process personal information (akin to a "data processor" under the GDPR) shall take necessary measures to safeguard the security of the processed personal information, and assist personal information processors in fulfilling the obligations under PIPL. By way of reference, the Personal Information Security Specification and relevant industry good practices that the entrusted persons may need to comply with include:[12]

- Provide proof materials and compliance documents on network and data security capabilities to cooperate with personal information protection impact assessments and auditing of the personal information processor

- Assist the personal information processor in responding to the requests of the individuals whose personal information is processed

- Meet other obligations as set out in the agreement between the entrusted party and the personal information processor (this is likely to be in the form of a data processing agreement)

Legal Responsibilities

Increased penalties

According to Article 66 of PIPL, if personal information is processed in violation of PIPL or without fulfilling personal information protection duties in accordance with PIPL, the personal information processor may face a penalty of not more than CNY50 million, or 5% of its annual revenue of the last year.

The fine is of a similar amount with fines under other legislation in China, such as the Anti-Monopoly Law.

Private right of action

Article 50 of PIPL stipulates that individuals may file a lawsuit if personal information processors refuse their requests to exercise their rights under PIPL. Further, Article 70 provides that if a personal information processor has infringed on the rights and benefits of a large number of individuals, consumer organizations stipulated by law or organizations designated by relevant authorities can file a lawsuit.

Although the feasibility of such litigation in practice remains to be seen, such provisions of PIPL, together with the E-Commerce Law and the Consumer Rights Protection Law, will open the door to legal proceedings in cases of infringement of personal information rights, which in turn has the potential to bring litigation pressure on companies. How to cope with such compliance and litigation pressures will be an important challenge for companies in the future.

Key Takeaways

In summary, PIPL inherits and synthesizes the provisions of previous laws, regulations, and drafts on personal information protection, while adding a number of new elements by drawing on wide social concerns and foreign legislative precedents. The adoption and entry into force of PIPL could lead to the introduction of a large number of regulations, standards, and other rules, as well as provide a legal basis for the practices of law enforcement and judicial authorities, many of which are already underway.

For companies in relevant industries (e.g., technology, payments, finance, health and medicine, and gaming), the adoption of PIPL will undoubtedly increase compliance and even litigation costs. However, details like the special rules for small-scale personal information processors suggest that the legislators have taken into account the practical difficulties faced by businesses, and the room for interpretation reserved in many provisions of the law will likely be adjusted with practice experience. Companies in relevant industries should now take the following compliance steps:

- Improve the consent forms for personal information collection, set up a mechanism for obtaining separate consent, and revise the privacy policy to incorporate other legal bases for personal information collection
- Enhance the personal information security mechanism and implement a hierarchical protection system for sensitive personal information
- Reconsider the application of tools such as automated decision-making
- Review contracts and internal arrangements related to personal information cross-border transfers
- Revise policies related to the collection and use of employees' personal information

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Hui Xu
hui.xu@lw.com
+86.10.5965.7023
Beijing

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Bianca Lee
bianca.lee@lw.com
+852.2912.2781
Hong Kong

This *Client Alert* was prepared with the assistance of Zurui Yang in the Beijing office of Latham & Watkins.

You Might Also Be Interested In

China Issues New Regulations to Protect the Critical Information Infrastructure

China's New Data Security Law: What to Know

Extensive Changes to Singapore's Data Protection Regime Take Effect

Hong Kong Considers Sweeping Changes to Privacy Laws

Endnotes

[1] Unless otherwise specified, "First Draft" and "Second Draft" mentioned here refer to the First Draft and Second Draft of the Personal Information Protection Law.

[2] Unless otherwise specified, the Articles mentioned here refer to the Articles of the Personal Information Protection Law.

[3] In the First Draft and Second Draft, the principle of necessity was stipulated in Article 6, but moved into Article 5 in the final version.

[4] According to Art. 1036 of Civil Code, a personal information processor who reasonably process information that the information subject has disclosed on his or her own, or that has otherwise been lawfully disclosed shall not be subject to civil liability, except to the extent that the information subject has expressly refused the processing, or the personal information is processed in a manner that infringes upon the subject's substantial interests.

[5] Please refer to Han Kun Law Offices, *A New Chapter in the Spotlight: A Brief Overview of the Personal Information Protection Law*, August 22, 2021. See https://mp.weixin.qq.com/s?__biz=MjM5ODM3MzU4Mg==&mid=2653095499&idx=1&sn=35f938bbd687e16db5ff264f4269bcbf&chksm=bd1c17ea8a6b9efc5c727061243cd2352b3092b28463cf34564867757940a7bc8b624b92f4a6&mpshare=1&scene=24&srcid=0821xzA1K4eTUHFD9cdMaFQe&sharer_sharetime=1629528813210&sharer_shareid=a88aafa3571578919c254d9190b16ce8&ascene=14&devicetype=android-29&version=28000a3d&nettype=WIFI&abtest_cookie=AAACAA%3D%3D&lang=zh_CN&exportkey=A0f0NwTlkkxqnQ3tpCq4JYM%3D&pass_ticket=h2BcvOF83vmFPVAGh2aIrAyaYgmrLbZGuIBcasoQ%2Bk4xq8cw%2FzU5TRz2SX2OKZQ3&wx_header=1.

[6] For example, in a recent case at a court in Hangzhou, Zhejiang, the online hotel booking platform C-trip was convicted of false advertising, price fraud and excessive collection of personal information for providing a VIP user inflated prices (July 2021). See https://www.pkulaw.com/pal/a3ecfd5d734f711dd459d6fcb85ee21ee7a45abb6f2cd7fabdfb.html?keyword=%E6%9D%80%E7%86%9F.

[7] *Supra* note 5.

[8] See https://mp.weixin.qq.com/s/GZkFr4DVxPPRvp0_RP8mAQ.

[9] See Announcement on Concentrated Rectification of Camera Peeping and Other Black Industry, http://www.gov.cn/xinwen/2021-06/12/content_5617355.htm.

[10] *Supra* note 5.

[11] Such as National Health Care Big Data Standards, Security and Service Management Approach (Trial) published by National Health Commission (took effect in July 2018) and Regulations on Strengthening Confidentiality and File Management Related to Securities Issuance and Listing Abroad published by China Securities Regulatory Commission, State Secrecy Administration and State Archives Bureau (took effect in October 2009).

[12] Please refer to Zhong Lun Law Firm, *Panorama Analysis on the Personal Information Protection Law: Help the companies enter a new era of Personal Information Protection in China*, August 21, 2021. See http://www.zhonglun.com/Content/2021/08-21/0130117987.html.