Personal Information Protection Law of the People’s Republic of China—Overview

People’s Republic of China (PRC) Passes Law Setting Forth Rules Governing the Handling of Personal Information, Set to Go Into Effect November 1, 2021

SUMMARY

On August 20, 2021, the Standing Committee of the 13th National People’s Congress passed the Personal Information Protection Law of the People’s Republic of China (“PIPL”). The new law, which is set to go into effect on November 1, 2021, sets forth rules governing the handling of personal information and defines certain individual rights with respect to personal information. PIPL differs significantly from several other comprehensive data protection laws, such as the European Union’s General Data Protection Regulation (“GDPR”). In particular, PIPL limits the legal bases for processing personal information (and does not include “legitimate interests” as a basis for processing information), contains heightened consent requirements for certain types of personal information handling (such as sharing personal information with other entities that handle personal information) and imposes special cross-border data transfer rules under certain circumstances (such as where the amount of personal information being processed reaches a certain threshold to be determined by the PRC national cyberspace authority (the “Cyberspace Authority”)). This memo presents a brief informational overview of the new rules.

Key provisions of PIPL include the following:

- **Individual Consent:** Organizations and individuals that autonomously decide the purposes and methods of “handling” personal information (“PI Handlers”) may only handle personal information with the consent of the individual whose information is being handled, or otherwise pursuant to one of six other enumerated circumstances (described further below).

- **Notice Requirements:** PI Handlers must notify individuals of (1) the PI Handler’s name and contact information; (2) the purpose, handling methods, categories and retention period with respect to the personal information being handled; (3) methods and procedures for individuals to...
exercise the rights provided in PIPL; and (4) any other items that individuals are required to be notified of under applicable laws or regulations. PI Handlers must further notify individuals of a change in any of the foregoing.³

- **Applicability Outside the PRC:** PIPL applies to activities outside the PRC involving the handling of personal information of natural persons based in the PRC where (1) the purpose is to provide products or services to natural persons within the PRC; (2) analyzing or assessing activities of natural persons within the PRC; or (3) provided by other circumstances under applicable laws or regulations.⁴ PI Handlers outside the PRC that are subject to PIPL face certain additional requirements, including the obligation to establish a dedicated entity or appoint a representative within the PRC to be responsible for personal information handling.⁵

- **Cross-Border Transfer:** PI Handlers that need to transfer personal information outside the borders of the PRC must comply with one of four sets of conditions, one of which provides that such information may be transferred pursuant to a standard contract promulgated by the Cyberspace Authority. In addition, PI Handlers must adopt necessary measures to ensure that parties outside the PRC that receive personal information comply with the standard of personal information protection provided under PIPL.⁶

- **Penalties:** PIPL provides for injunctive and monetary penalties in the event of violations, including corrective actions, confiscation of any unlawful income and suspension of any personal information handling services. Where violators refuse to correct a violation, fines of up to ¥1 million (USD$160,000)⁷ may be imposed, and persons directly responsible for personal information handling are subject to fines of between ¥10,000 and ¥100,000 (or between USD$1,600 and USD$16,000). In circumstances involving “grave” violations of PIPL, violators are subject to fines of up to ¥50 million (or over USD$7.8 million) or 5% of annual revenue. Fines for persons directly responsible for grave violations of PIPL range from ¥100,000 and ¥1 million (or between USD$16,000 and USD$160,000).⁸

---

**OVERVIEW**

**General Provisions and Applicability**

PIPL broadly applies to the “handling” of personal information, where “handling” includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information. “Personal information” includes any information related to identified or identifiable natural persons, but does not include information that has been anonymized such that it is impossible to identify a natural person and the personal information is “impossible to restore.”⁹

PIPL applies to the handling of personal information “within the borders” of the PRC. The law also applies in the following circumstances where personal information of natural persons within the borders of the PRC is being handled outside the PRC: (i) where the purpose is to provide products or services to natural persons within the borders of the PRC; (ii) where analyzing or assessing activities of natural persons inside the borders of the PRC; or (iii) as otherwise provided under applicable laws or regulations.¹⁰

The law contains certain general provisions to define and safeguard the rights of individuals with respect to their personal information. Such provisions include restrictions on the handling of personal information in a manner that is misleading, swindling or coercive, and that personal information may only be handled with a clear and reasonable purpose. In addition, the collection of personal information must be limited to the smallest scope of information needed to achieve the handling purpose.¹¹
PIPL will be further implemented through regulations and standards to be developed by the Cyberspace Authority. That department will also formulate specialized rules for new technologies and applications, support research and development, including in the area of electronic identity authentication, and support organizations that develop personal information protection evaluation and certification services.\textsuperscript{12}

**Handling of Personal Information**

*Individual Consent and Other Legal Bases for Handling Personal Information*

PIPL provides that PI Handlers may only handle personal information where the individual’s consent has been obtained, and such consent has been provided voluntarily and explicitly by individuals who are fully informed of the personal information handling. In addition, PI Handlers must obtain new consent from individuals upon any changes in the purpose of personal information handling, the handling method or the categories of personal information that will be handled. An individual may revoke consent, and PI Handlers may not refuse to provide products or services to individuals who have revoked their consent. The revocation of an individual’s consent does not affect the personal information handling activities undertaken before consent was revoked.\textsuperscript{13}

If an individual’s consent has not been obtained, personal information may only be handled under the following circumstances:

- **Contractual:** Where necessary to conclude or fulfill a contract in which the individual is an interested party or to conduct human resources management activities in accordance with applicable labor rules and lawfully concluded collective contracts.
- **Statutory:** Where necessary for the PI Handler to fulfill statutory obligations and responsibilities.
- **Public Health:** Where necessary to respond to sudden public health incidents or to protect natural persons’ lives and health, or the security of their property, under emergency conditions.
- **Public Interest:** Within a reasonable scope to implement news reporting, public opinion supervision and other such activities for the public interest.
- **Lawful Disclosure:** Within a reasonable scope where the relevant personal information has been disclosed by the individuals themselves or otherwise already lawfully disclosed.
- **Applicable Law:** In other circumstances provided for by laws and administrative regulations.

Notably, PIPL does not provide for the handling of personal information for the “legitimate interests” of the PI Handler, which is commonly used by companies to process data under the GDPR in a number of contexts, such as corporate transactions.\textsuperscript{14}

**Notice Requirements**

Except as otherwise provided in accordance with applicable law or under emergency circumstances, PI Handlers must provide individuals with notice of the following items in clear and easily understood language:

- **PI Handler Info:** Name and contact information of the PI Handler.
Handling Information: The purpose of the personal information handling, the handling methods, the categories of handled personal information and the retention period.

PIPL Rights: The methods and procedures for individuals to exercise the rights provided under PIPL.

Other Applicable Law: Other items required to be provided to individuals under applicable laws or administrative regulations.\textsuperscript{15}

Other Handling Rules

Other notable handling rules include the following:

Retention Period: PI Handlers must establish retention periods for personal information that are generally the shortest period necessary to realize the purpose of the personal information handling.\textsuperscript{16}

Corporate Transactions: Where it is necessary to transfer personal information due to mergers, separations, dissolution, declaration of bankruptcy and other such reasons, PI Handlers must notify individuals of the receiving party’s name and contact information. PIPL does not specify within what time period such notification must be provided (e.g., after signing, after closing). The successor entity or receiving party must continue to fulfill the PI Handler’s duties with respect to the personal information that is transferred. Where the successor entity or receiving party changes the original handling purpose or method, such party must notify the individual again in accordance with PIPL.\textsuperscript{17}

Vendors: PI Handlers that provide personal information to vendors must enter into an agreement with the vendor that states the purpose for the personal information handling, the duration of such handling, the personal information handling method, the categories of personal information disclosed and measures to safeguard the personal information and the rights and duties of the parties. If such agreement is terminated or no longer in effect, the vendor must return the personal information to the PI Handler or delete it. Without the consent of the PI Handler, the vendor may not further provide the personal information to other vendors.\textsuperscript{18}

Sharing Personal Information: PI Handlers must generally obtain the individual’s consent to share their personal information with other PI Handlers (as distinct from providing personal information to vendors pursuant to an agreement (see above)). This consent requirement could pose an obstacle to a number of corporate activities, such as joint marketing and other data-sharing arrangements. In addition, such PI Handlers must notify the individual of the recipient’s name and contact information, handling purpose and method and personal information categories.\textsuperscript{19}

Automated Decision-Making: PI Handlers may engage in automated decision-making with respect to personal information, which is defined as utilizing computer programs to automatically analyze or assess personal behaviors, interests, financial health and credit, and making decisions based on such analysis. PI Handlers may not engage in unreasonable differential treatment of individuals based on such automated decision-making, including price discrimination. PI Handlers that engage in information push delivery or commercial sales to individuals based on automated decision-making shall offer the option of not targeting an individual’s characteristics or a convenient method for individuals to refuse such automated decision-making.\textsuperscript{20}

Individual Rights

PIPL defines certain individual rights with respect to personal information handling, and PI Handlers must develop convenient mechanisms to accept requests from individuals to exercise their rights.\textsuperscript{21} The rights granted to individuals under PIPL include:
• **Right to Know:** Individuals broadly have the right to know and make decisions relating to their personal information, and further have the right to limit or refuse the handling of their personal information by others, unless laws or regulations state otherwise.22

• **Right to Consult:** Individuals have the right to consult and copy their personal information except where applicable laws or regulations provide for the confidentiality of such information. Where individuals so request to consult or copy their personal information, PI Handlers must timely respond to such requests.23

• **Right to Portability:** Individuals have the right to request that their personal information be transferred to a PI Handler meeting the conditions set out by the Cyberspace Authority, and PI Handlers must provide a channel to conduct such transfer.24

• **Right to Correct:** Individuals have the right to request PI Handlers correct or complete their personal information. Upon such requests, PI Handlers must verify the personal information and correct or complete it in a timely manner.

• **Right to Delete:** PI Handlers must delete an individual’s personal information in one of five circumstances, including where the individual revokes their prior consent for handling the personal information. Other circumstances in which PI Handlers must delete an individual’s personal information include where (1) the handling purpose has been achieved, is impossible to achieve or the personal information is no longer necessary to achieve the handling purpose, (2) the PI Handler has ceased to provide products or services or the retention period applicable to such personal information has expired, (3) personal information is being handled in violation of applicable laws or regulations and (4) as dictated by other applicable laws or regulations.25

PIPL further provides that individuals have the right to request PI Handlers explain their personal information handling rules.26 Where PI Handlers reject individuals’ requests to exercise their rights under PIPL, PI Handlers must explain the reasons for rejection. Individuals may file a lawsuit with a People’s Court in the PRC if their requests are denied.27 This private right of action is more expansive than jurisdictional provisions of several other comprehensive data protection laws, which may only permit appeals and complaints to be filed with the appropriate data protection authority.

**Cross-Border Transfer**

PI Handlers that need to transfer personal information outside the borders of the PRC must meet certain requirements before doing so. First, such PI Handlers must notify individuals about the data transfer. Such notice must include the foreign data recipient’s name, contact method, purpose of handling personal information, handling methods and categories of personal information disclosed, as well as procedures for the individual to exercise their rights under PIPL with the foreign data recipient. PI handlers must also obtain individuals’ separate consent to transfer the relevant personal information (without exception).28

While it is unclear how the notice and consent requirements will be implemented in the cross-border data transfer context, many companies routinely transfer data outside the jurisdiction in which the data was originally collected for a variety of purposes, and it might be difficult to notify and obtain the consent of each and every data subject whose personal information is so transferred.

In addition, PI Handlers seeking to transfer personal information outside the borders of the PRC must meet one of the following four conditions:
Personal Information Protection Law of the People’s Republic of China—Overview
October 27, 2021

- Security Assessment: Passing a security assessment developed by the Cyberspace Authority.
- Governmental Certification: Undergoing personal information protection certification conducted by a specialized body in accordance with certain provisions set by the Cyberspace Authority.
- Standard Contract: Entering into a contract with the foreign entity receiving the personal information in accordance with a standard contract formulated by the Cyberspace Authority.
- Other Conditions: Other conditions as set forth under applicable laws or regulations or by the Cyberspace Authority.

PRC authorities are required to handle any requests for personal information stored within the PRC from foreign judicial or law enforcement authorities. PI Handlers must not provide personal information to such foreign authorities without approval from the applicable PRC authorities. Treaties or international agreements to which the PRC has acceded may contain additional conditions on the transfer of personal information outside the PRC that may apply.29

Special Duties of PI Handlers

General Requirements
PI Handlers must adopt certain measures to prevent unauthorized access to, and leaks, distortion or loss of, personal information. This includes forming internal management structures and operating rules, implementing categorized management of personal information, implementing technical safeguards such as encryption de-identification, conducting security education and training, and formulating incident response plans. PI Handlers must also engage in regular audits of their personal information handling activities.30

PI Handlers Outside the PRC
PI Handlers outside the PRC that are subject to PIPL must establish a dedicated entity or appoint a representative within the borders of the PRC. That entity or representative will be responsible for personal information handling matters and must notify or register with the relevant PRC regulator.31

Personal Information Protection Impact Assessments
PI Handlers must conduct personal information protection impact assessments before handling personal information when:

- handling “sensitive” personal information (as further described below);
- using personal information to conduct automated decision-making;
- entrusting personal information to vendors or other PI Handlers;
- transferring personal information outside the PRC; and
- conducting any other personal information handling activities with a “major influence” on individuals.

The personal information protection impact assessment must contain certain content, such as whether the personal information handling purposes and methods of handling are lawful, legitimate and necessary; the
influence of the personal information handling on individuals' rights and interests and the security risks; and whether any protective measures are suitable to the risk involved in the personal information handling. PI Handlers must preserve personal information protection impact assessments for at least three years.\textsuperscript{32}

**Data Breaches**

Where a personal information leak, distortion or loss has or may have occurred, PI Handlers must immediately adopt remedial measures and notify the relevant PRC departments or regulators and the affected individuals.

PI Handlers that adopt measures that effectively avoid potential harm created by such data breaches are permitted to not notify individuals, though the relevant state departments or regulators may nonetheless require the affected individuals to be notified if they believe harm may have been caused by the data breach.\textsuperscript{33}

**Other Duties**

Additional requirements may apply to certain PI Handlers, including PI Handlers that handle an amount of personal information reaching a certain threshold to be set forth by the Cyberspace Authority, and PI Handlers that provide important Internet platform services with large numbers of users and who have “complex” (which is undefined in the PIPL) business models.\textsuperscript{34}

**Special Rules**

PIPL contains certain provisions to address “sensitive” categories of personal information and the handling of personal information by state organizations.

Sensitive personal information includes personal information that, if improperly disclosed, could harm the dignity of the individual, such as biometric information, health information, financial account information and location tracking information. PIPL sets forth heightened consent and notice requirements with respect to the handling of sensitive personal information. In addition, PIPL requires the consent of a parent or guardian to handle the personal information of minors under the age of 14.\textsuperscript{35}

PIPL expressly applies to the handling of personal information by state organizations.\textsuperscript{36}

**Enforcement and Penalties**

PIPL provides for enforcement by the Cyberspace Authority, relevant departments of the State Council of the PRC and relevant departments of local governments at the county level or above.\textsuperscript{37} Any organization or individual has the right to file a complaint about unlawful personal information handling activities with the appropriate authority, which must be investigated promptly.\textsuperscript{38} Investigations may involve interviews of relevant parties, reviewing contracts and other records, conducting on-site inspections and inspecting equipment and articles relevant to personal information handling activities.\textsuperscript{39}
Upon determining that a violation of PIPL has occurred, authorities may order PI Handlers to correct alleged violations of PIPL, confiscate unlawful income and suspend or terminate service to address violations of the law. Where a PI Handler refuses to take corrective action, PIPL provides for an additional fine of up to ¥1 million (USD$160,000) to be imposed on the organization and of between ¥10,000 and ¥100,000 (or between USD$1,600 and USD$16,000) on individuals directly responsible for the personal information handling. In the event of grave violations, PIPL provides that fines of up to ¥50 million (or USD$7.8 million) or 5% of annual revenue may be imposed. The individuals directly responsible for such violations are subject to fines of between ¥100,000 and ¥1 million (or between USD$16,000 and USD$160,000).

PIPL further provides that PI Handlers carry the burden of proof to demonstrate they are not at fault where the personal information handling infringes upon personal information rights and interests, and results in harm. If PI Handlers cannot prove they are not at fault in such circumstances, they must pay compensation and take responsibility for the infringement.

**CONCLUSION**

Businesses that handle the personal information of natural persons based in the PRC, including those businesses outside of the PRC whose activities fall within the scope of PIPL, should closely review the new rules set forth in PIPL and prepare for the law to take effect on November 1, 2021. These preparations may include drafting privacy notices and consent forms, developing policies and procedures for individuals to exercise their rights, reviewing and revising vendor agreements, developing personal information protection impact assessments and updating incident response plans. Failure to comply with PIPL may result in injunctive or substantial monetary penalties, including fines for individuals that are directly responsible for PIPL violations.


U.S. dollar amounts referenced herein are current as of the date of this publication.

People’s Information Protection Law of the People’s Republic of China—Overview
October 27, 2021
ENDNOTES CONTINUED

34 PIPL arts. 40, 58.
35 PIPL arts. 28-31.
36 PIPL art. 33.
37 PIPL art. 66.
38 PIPL art. 65.
39 PIPL art. 63.
40 PIPL art. 66.
41 PIPL art. 66.
42 PIPL art. 69.
SULLIVAN & CROMWELL LLP

ABOUT SULLIVAN & CROMWELL LLP
Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP
This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.