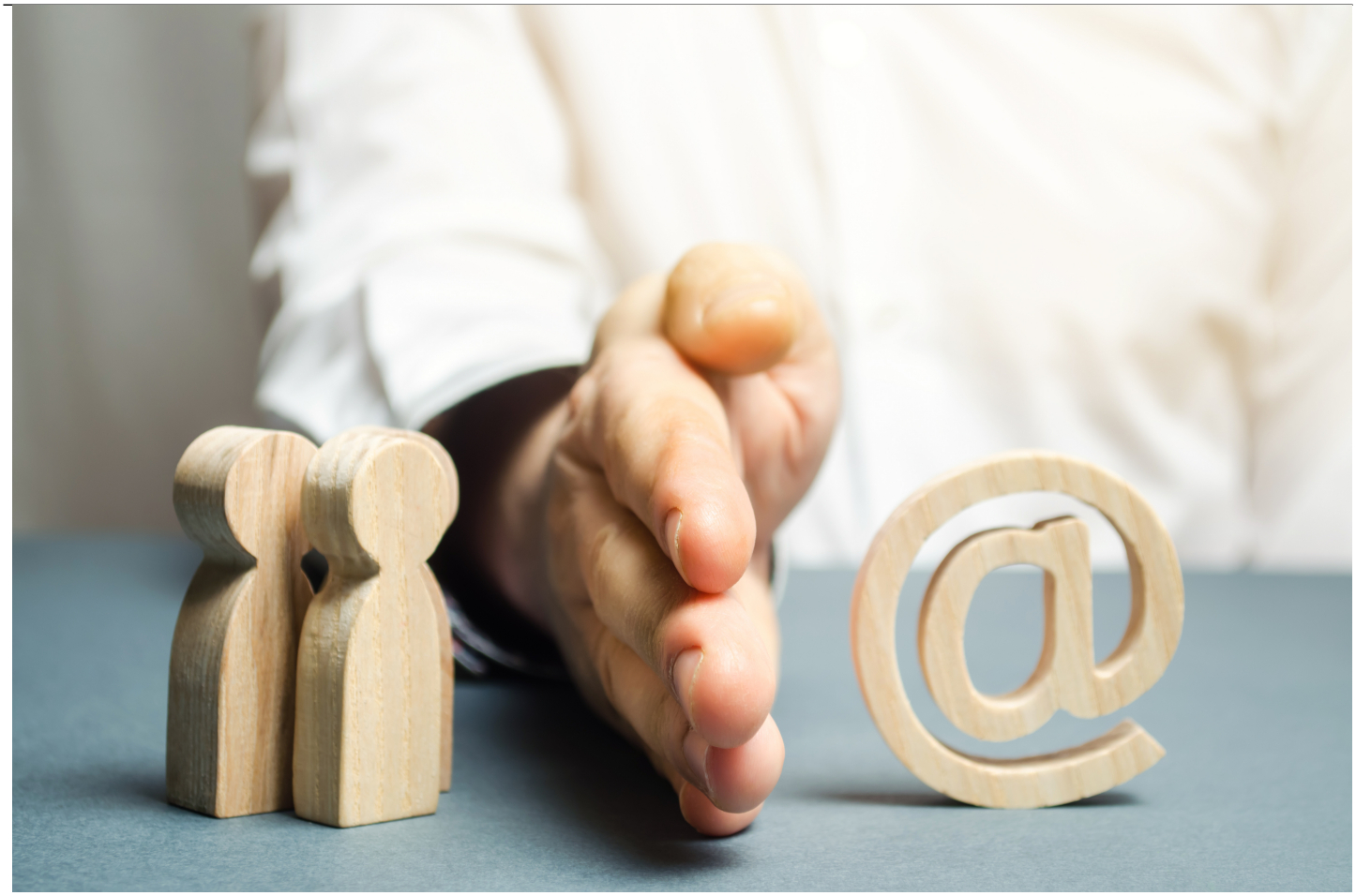
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Everything You Need to Know About China’s Personal Information Protection Law

Technology, Privacy, and eCommerce



Cheat Sheet

- **China’s first privacy law.**The country adopted many of the EU and UK General Data Protection Regulation (GDPR) requirements in its new Personal Information Protection Law (PIPL).
- **When outside China.** Certain conditions must be met when the personal information on Chinese individuals to be handled is beyond the country’s borders.
- **No clear guidance on operationalizing management of individual rights.** Responses must be handled “in a timely manner” — there is no mention of a delayed response scenario.

However, if entities reject individuals' requests to exercise their rights, individuals may file a lawsuit.

- **Personal information impact assessment.** Handlers must document the effect of reviewing the privacy information would have on the individual.

The first comprehensive data protection law in the People's Republic of China (China) was adopted by the National People's Congress (NPC) on August 20, 2021, with little time left for compliance preparation before it is enforced. Known as the Personal Information Protection Law (PIPL), it took effect on November 1, 2021.

It is easy to see the similarities to and differences from other national/multinational omnibus privacy laws, like the European Union's or the United Kingdom's General Data Protection Regulation (GDPR). China adopted many of the concepts of GDPR, such as individual rights, vendor management requirements, and data breach notification.

It is easy to see the similarities to and differences from other national/multinational omnibus privacy laws, like the European Union's or the United Kingdom's General Data Protection Regulation (GDPR).

Core data protection principles like purpose limitation, transparency, and data quality are also part of the law. As to data retention, the law spells out that "the shortest time necessary to achieve the purposes" is to be maintained. Accountability requirements are also included with the PIPL stating that "personal information handlers," i.e., data controllers, also known as just handlers, "shall take necessary measures to ensure that personal information handling activities comply with the provisions of laws and administrative regulations."

In addition, PIPL includes obligations for risk assessments and cross-border transfers — only allowed if "truly needed" — and then only if appropriate contracts are in place and/or a prescribed security assessment is executed. The extraterritorial provisions may also seem familiar, as entities must appoint a local representative if they do not have an entity established in China. Lastly, enforcement is entrusted to the Cybersecurity Administration of China, which will also be allowed to impose fines. This, and much more, are detailed below.

Fundamentals and key definitions

PIPL applies to “the activities of handling the personal information of natural persons within the borders of the People’s Republic of China” (Article 3). Further, processing (“handling” as the PIPL translation refers to it) of personal information outside China on individuals in China is also covered if one of three conditions is met:

- When the purpose is to provide products or services to natural persons inside the borders;
- When analyzing or assessing activities of natural persons inside the borders is being done;
- Other circumstances provided in laws or administrative regulations.

There are key definitions, but, in general, there are not very many definitions provided in PIPL:

- Personal information is defined as “all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling” (Article 4).
- Handling is very broad and includes “collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.” (Article 4).
- “Personal information handler” refers to organizations and individuals who engage in personal information handling activities or autonomously decide handling purposes (Article 75).

Exceptions

There are few, if any, exceptions to PIPL for types of information or categories of organizations. One exception is similar to GDPR in that PIPL “does not apply to natural persons handling personal information for personal or family affairs” (Article 72). There is also an exception to PIPL for government agencies for statistical and archival purposes, but only where those activities should follow the applicable law. There are some other exceptions built into PIPL for certain requirements based on other laws, none of which are named, but where appropriate, will be addressed in this white paper.

Handlers may, within a reasonable scope, use personal information that has already been disclosed by the person themselves or otherwise lawfully disclosed, except where the person clearly refuses. But if this information has a major influence on individual rights and interests, the handler shall obtain personal consent in accordance with PIPL.

Principles

Personal information must be handled (processed) by following certain principles and cannot be processed in “misleading, swindling, coercive, or other such ways” (Art. 5)., including:

- Legality;
- Propriety;
- Necessity;
- Sincerity;
- Transparency (Article 7); and
- Quality & Accuracy (Article 8).

In addition, there must be a clear and reasonable purpose for processing the personal information and all processing shall be limited to that purpose using a method with the smallest influence on individual rights and interest. Collection of personal information shall be limited to the minimum necessary for the purpose. Excessive data collection is prohibited. Further, the accuracy of the information is important to assure there are no adverse impacts to individuals from inaccurate or incomplete information (Article 8).

> ... There must be a clear and reasonable purpose for processing the personal information and all processing
> shall be limited to that purpose using a method with the smallest influence on individual rights and interest.

No one, entity or person, is permitted to illegally collect, use, process, or transmit an individual’s personal information, or illegally sell, buy, provide, or disclose an individual’s personal information, or engage in personal information handling activities that expose national security or the public interest (Article 10).

Personal information handling rules

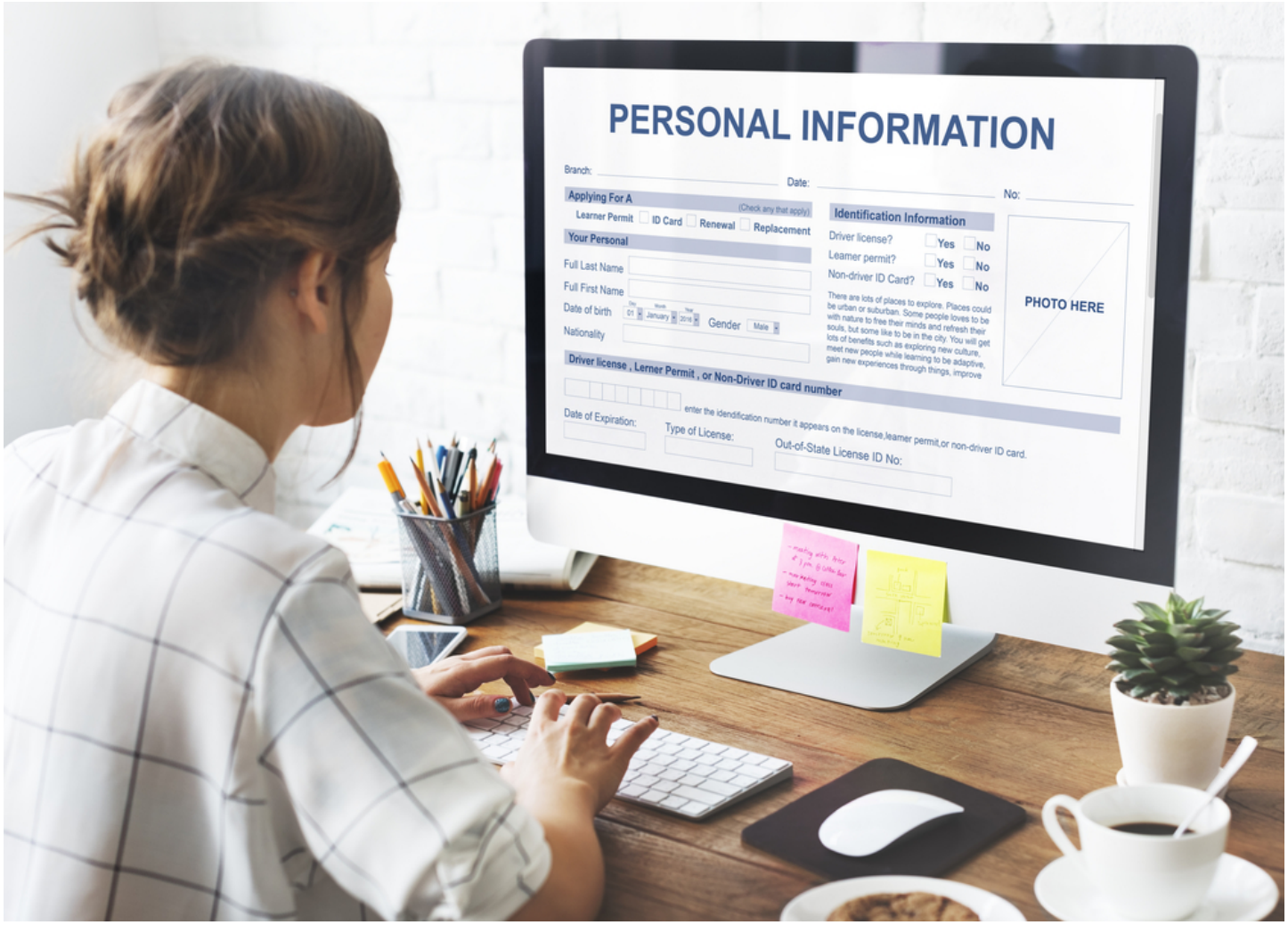
PIPL provides for specific rules of handling personal information. There are only six circumstances explicitly listed in PIPL, plus allowance for others that are otherwise required by law:

- Obtaining individuals’ consent;
- When necessary to conclude or fulfill a contract in which the individual is an interested party

or when necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded contracts;
- When necessary to fulfill statutory duties and responsibilities or statutory obligations;
- When necessary to respond to sudden public health incidents or protect natural persons' lives and health or the security of their property in an emergency;
- Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;
- When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this law; and
- Other circumstances provided in laws and administrative regulations.

At this time, there is no concept of processing personal information based on legitimate interest. If one of these reasons above is not present (and clearly documented), the handlers will need to seek consent for processing personal information. Consent is covered further below in special processing.

Personal information is only permitted to be retained for the period required to accomplish the stated purpose. (Article 19).



Sensitive personal information

Handlers managing sensitive personal information carry additional obligations. Sensitive personal

information may only be processed for a specific purpose and need, with strict protective measures (Article 28).

> Sensitive personal information may only be processed for a specific purpose and need, with strict protective measures (Article 28).

“Sensitive personal information” means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons, grave harm to personal or property security, 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.

Separate consent is needed for sensitive personal information (Article 29). If there are other laws addressing this information, those laws must be followed.

Some of the obligations for handling sensitive personal information are for notice provisions and relate specifically to handling the data of individuals under the age of 14. If Handlers process the personal information of minors under the age of 14, they need to obtain the consent of the parent or other guardian of the minor (Article 31). In addition, they need to develop specialized rules (internal policies and processes) for handling this information.

Individual rights

Like most privacy laws, PIPL provides individuals with certain rights (Chapter IV). The PIPL provides a specific list of rights, but a thorough reading of PIPL reveals that there are other rights that are also specified for individuals.

> The PIPL provides a specific list of rights, but a thorough reading of PIPL reveals that there are other rights that are also specified for individuals.

Except where applicable laws say otherwise, individual rights include the following:

- Transparency and notice (Article 17),
- Know if an entity is processing their personal information (Article 44),
- Decide if and how their personal information is processed (Article 44),
- Limit or refuse data processing (Article 44),
- View and copy (exceptions are provided, mainly if restricted by other laws) (Article 45),
- Portability (Article 45),
- Correction and amendment (Article 46),
- Deletion (Article 46), and
- To know (and have explained) the personal information handling rules, if there are any (Article 48).

But individuals also have these rights:

- Non-discrimination for exercising rights (Article 16),
- To know and refuse automated decision-making activities (Article 24),
- Refuse targeted ads done by automation (be careful how this impacts cookies), and

- Consent to cross-border transfers (Article 39).

It is noted that portability is truly a porting requirement. PIPL provides in Article 45 that “where individuals request that their personal information be transferred to a personal information handler they designate, meeting conditions of the State cybersecurity and informatization department, personal information handlers shall provide a channel to transfer it.” No conditions have been provided by that department yet, so this is an area that requires clarification.

The right to deletion is allowed when handlers have not proactively deleted the personal information that they are required to delete. Handlers are required to delete personal information proactively under five conditions:

- The handling purpose has been achieved, is impossible to achieve, or the personal information is no longer necessary to achieve the handling purpose;
- Handlers cease the provision of products or services, or the retention period has expired;
- The individual rescinds consent;
- Handlers handled personal information in violation of laws, administrative regulations, or agreements; and
- Other circumstances provided by laws or administrative regulations.

If the retention period has not expired or deletion is not technically feasible, the handler may retain the data, but only for storage, and must continue to protect it. This is similar to the restriction of processing under GDPR.

Responding to individual requests

PIPL does not provide clear guidance on operationalizing management of individual rights. The requirement is to respond “in a timely manner” with no mention of a delayed response scenario. However, as mentioned above, if entities reject individuals’ requests to exercise their rights, individuals may file a lawsuit.

Handlers must establish convenient mechanisms for individuals to submit their requests. If handlers reject any rights requests, they shall provide an explanation (Article 50). However, individuals may file a right of action in court to enforce their rights (Article 50).

Deceased persons

When a natural person is deceased, their next of kin may, for the sake of their own lawful and legitimate interests, exercise the rights provided in PIPL relating to the personal information of the deceased, except where the deceased has arranged otherwise before death (Article 50).

Transparency (privacy notice)

Before processing personal information, handlers shall explicitly provide an accurate (truthful), clear, and understandable privacy notice (Article 17) that includes:

- The name or personal name and contact method of the personal information handler;
- The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period;
- Methods and procedures for individuals to exercise the rights including how to reach the data

protection officer (DPO);
- Other items that laws or administrative regulations provide shall be notified.
- Plus for sensitive personal information, handlers must also disclose the necessity and the influence on individuals' rights and interest except where permitted not to do so (Article 30).
- Cross-border transfers, currently or proposed in future, with separate consent.

If anything changes, including additional uses for the information or sharing the information outside the entity, handlers should amend the notice and notify individuals. In many cases, handlers will need to gain new consent from individuals.

If the handler has appointed a DPO, as addressed further below, the contact methods must also be publicly disclosed. Where handlers provide notice through development of personal information handling rules, the handling rules shall be made public and be convenient to read and store.

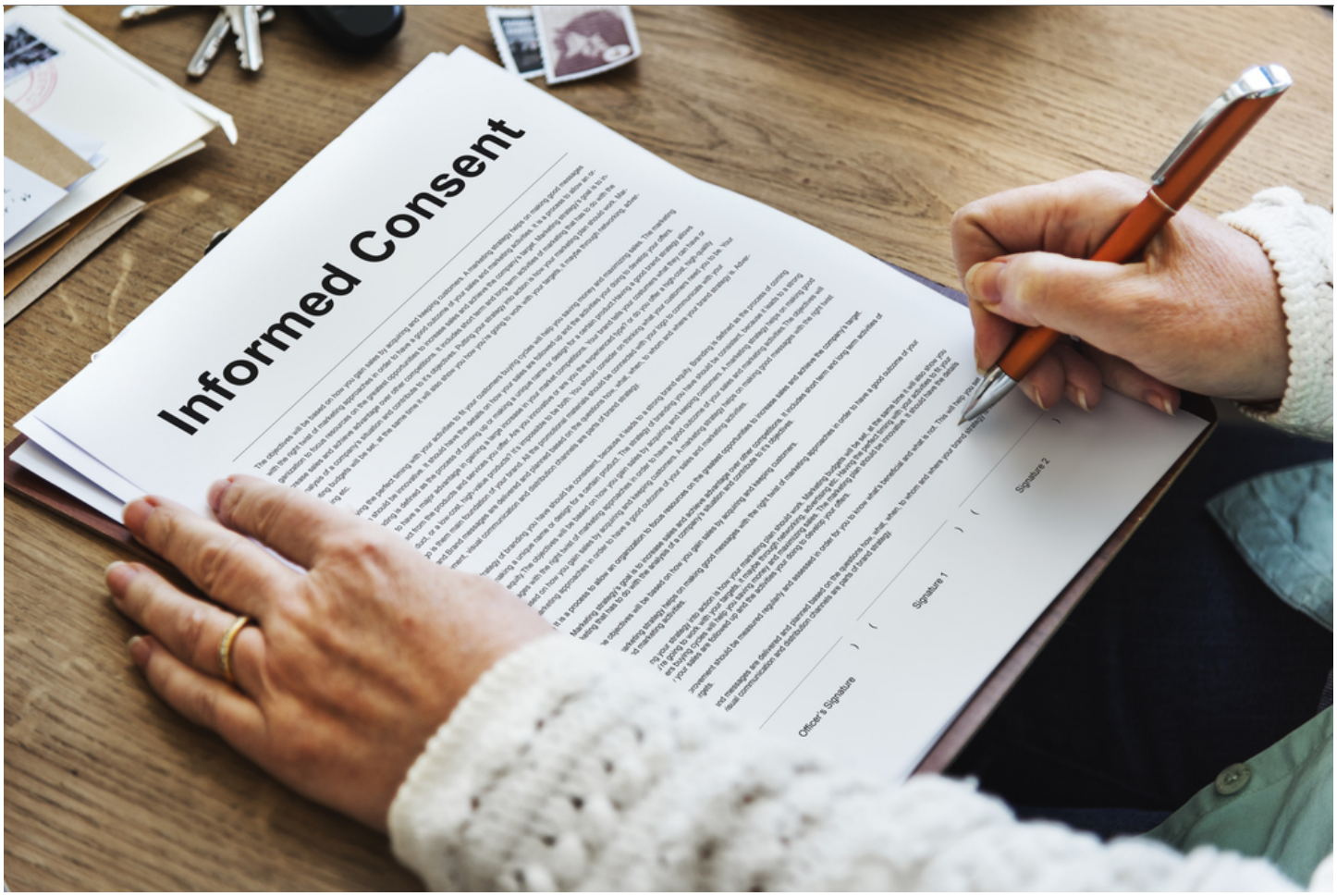
This notice is not required "under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary" (Article 18). Also, advance notice is not required if it is impossible to notify individuals in advance, such as in an emergency impacting someone's life, health, or security of their property. However, notice must be provided as soon as possible after the emergency.

The last right of non-discrimination is not new in the individual rights playbook. It has for example been included specifically in the California Consumer Privacy Act (CCPA). Individuals should not face discrimination in the provision of products or services on the basis of enforcing their rights. The only exception here would be if they refused to provide or revoked consent and the data is required to provide the service or product (Article 16).

> Individuals should not face discrimination in the provision of products or services on the basis of enforcing their rights.

Special Processing Activities

Four specific definitions, one of which (automated decision-making) was listed earlier under "personal information handling rules," are provided under Article 73 of the PIPL. The others are consent, de-identification and anonymization, and surveillance.



Consent

PIPL relies on consent quite prominently. If none of the processing purposes are present, such as for contracts, emergencies, public interest, legal compliance, or public information, then individuals must consent from the very first collection of their data. Handling sensitive personal data requires separate consent.

Consent must be fully informed, voluntary, and explicit (Article 14). Unless another law in China applies to consent, which must be followed, PIPL sets the requirements. If any changes occur, such as a new purpose for the data, a new way of handling the data, or collecting new categories of data, the individual must be informed in advance and must agree to such new or different data processing.

Along with consent, though, comes the revocation of consent (Article 15). Individuals must be able to revoke consent in a convenient manner. Revocation usually only impacts future use of the information, not the past use.

However, in cases in which it is possible to remove the past uses, clarification may be needed. For example, a person’s name would not be able to be removed from a printed list of attendees to a dinner, but where that list is posted on your website, that could likely be deleted.

As stated above in the rights, individuals who refuse to consent or revoke consent should not be refused service or products unless their data is specifically required to provide those services or products (Article 16).

Also, as mentioned above, although handlers may use personal information that has already been disclosed by the individual themselves or otherwise lawfully disclosed, they cannot use the data if the person clearly refuses. In addition, where there is a major influence on individuals' rights and interests, the handlers must obtain that person's consent prior to using this publicly disclosed information. A risk assessment is therefore likely to be required.

De-identification vs anonymization

"De-identification" refers to the process of personal information undergoing handling to ensure it is impossible to identify specific natural persons without the support of additional information whereas "anonymization" refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore. The former makes it hard to identify people, only possible with additional information. The latter means they cannot be identified any longer. This is very much like the definitions in GDPR.

Surveillance

PIPL prohibits the installation of image collection or personal identity recognition equipment in public venues unless for public security, when abiding by relevant State regulations, and if clear signs are posted indicating surveillance is in place. Collected personal images and personal distinguishing identity characteristic information can only be used for the purpose of safeguarding public security; it may not be used for other purposes, except where individuals' separate consent is obtained.

PIPL prohibits the installation of image collection or personal identity recognition equipment in public venues unless for public security, when abiding by relevant
state regulations, and if clear signs are posted indicating surveillance is in place.

Responsibilities of personal information handlers

The obligations on each party are similar to other nation's data privacy laws. Handlers (controllers) and their vendors (referred to as entrusted persons) must be bound by written contracts and are each responsible for only the measures allocated to them, which must be clearly documented. Handlers must also maintain the confidentiality of the data they process.

Handlers - privacy programs

Handlers are responsible for their processing activities and must adopt the necessary controls to safeguard the data (Article 9). Based on the processing activities, taking into account the purpose, method, categories of data, influence on individuals' interests and rights, and security risks, handlers must develop a privacy program with specific requirements (Article 51). Handlers must develop programs that address:

- Formulating internal management structures and operating rules, e.g., accountability mechanisms;
- Implementing categorized management of personal information, e.g., data classification;
- Adopting corresponding technical security measures such as encryption and de-identification;
- Reasonably determining operational limits for personal information handling, and
- Conducting regular security education and training for employees;
- Organizing security incident response plans; and
- Other measures provided in laws or administrative regulations.

Handlers should identify other laws or regulations to which they are subject, typically based on activities, such as healthcare or finance. Also, new laws are likely to develop along with the expected guidance under PIPL. Handlers are required to engage in regular audits of their program to make sure their processing and activities comply with the laws and regulations (Article 54).

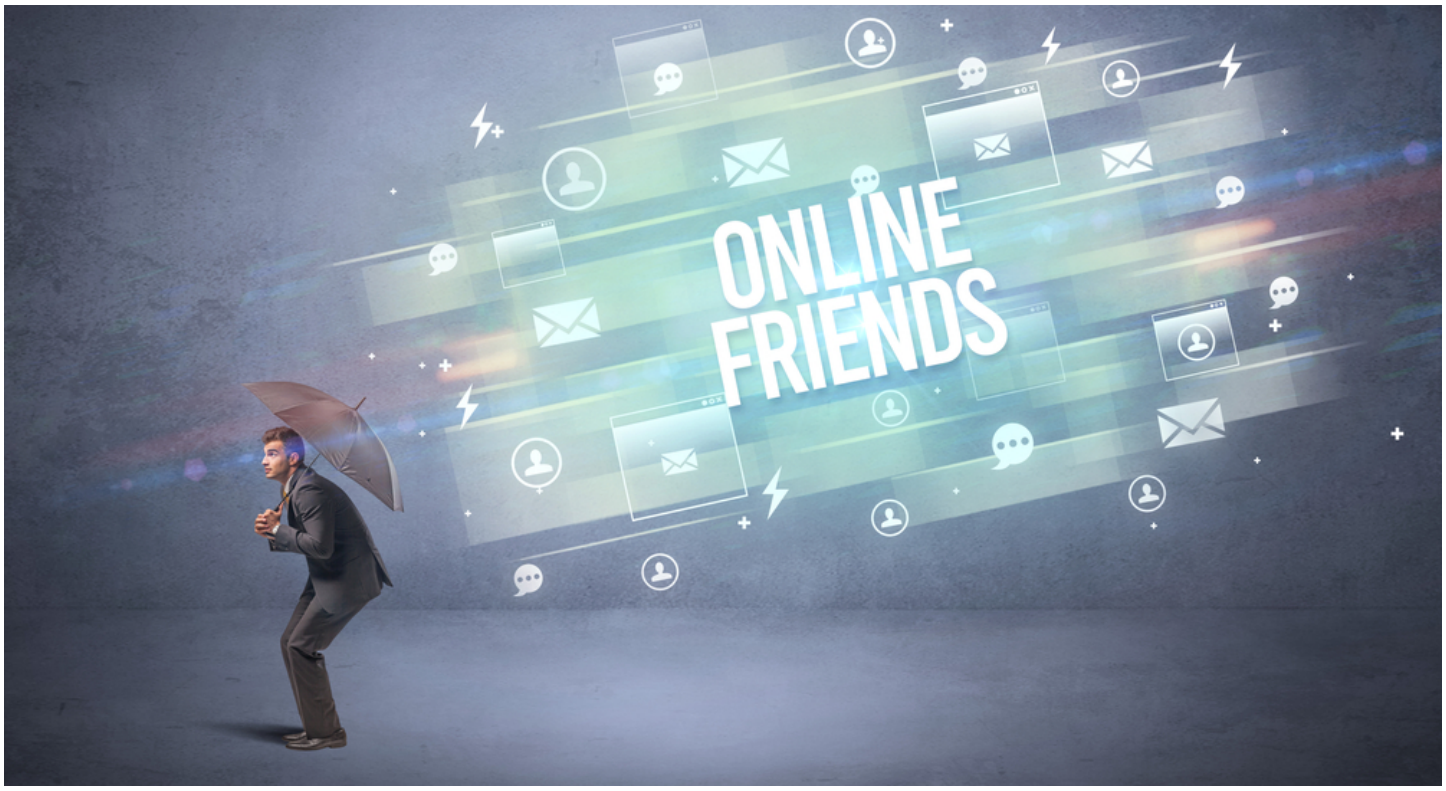
Joint handlers

Like many other laws, there is a concept of joint controllership or, in China, joint handlership. Joint handlers must agree on respective responsibilities between the two of them (or more) (Art. 20), but individuals may enforce their rights against either handler. Joint handlers bear joint liability.

Handlers that provide "important Internet platform services"

PIPL has special requirements for handlers that provide "important internet platform services, that have a large number of users, and whose business models are complex" (Article 58).

PIPL has special requirements for handlers that provide "important internet platform services, that have a large number of users, and whose business models are complex" (Article 58).



In addition to the programmatic steps above, these handlers must:

- Establish and complete personal information protection compliance systems and structures according to state regulations;
- Establish an independent body composed mainly of outside members to supervise personal information protection circumstances;
- Abide by the principles of openness, fairness, and justice, formulate platform rules, and clarify the standards for intra-platform product or service providers' handling of personal information and their personal information protection duties;
- Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information; and
- Regularly release personal information protection social responsibility reports and accept society’s supervision.

Although this term for important internet service platforms is not defined, this provision should be noted if it potentially applies. More guidance should be forthcoming on these requirements.

Data protection officers

Handlers managing quantities of personal data (the amount yet to be determined) must appoint a DPO who is responsible for supervising the processing activities and protection measures (Article 52). Handlers must register the DPO with the authorities along with how the DPO may be contacted. As mentioned above in the notice, the methods to reach the DPO must be readily available to individuals.

Representatives - handlers located outside China

Handlers who do not have an establishment in China must appoint a personal representative within China and register the representative and contact information with the authorities. The representative may be a person or entity (Article 53).

Impact assessments

Handlers must perform a documented personal information impact assessment before engaging in the following activities (Article 55):

- Handling sensitive personal information;
- Using personal information to conduct automated decision-making;
- Entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information;
- Providing personal information abroad; and
- Other personal information handling activities with a major influence on individuals.

Impact assessments must include (Article 56):

- Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary;
- The influence on individuals' rights and interests, and the security risks; and
- Whether protective measures undertaken are legal, effective, and suitable to the degree of risk.

Once documented, the impact assessments must be retained for at least three years.

Special requirements

For critical infrastructure providers and handlers who manage large quantities of data, they must store personal information locally. It is yet to be defined when a company falls under the definition. If they need to send the data outside China, they can only utilize the security assessment by the state cybersecurity and information department unless specific laws provide otherwise.

Security and data breach

Handlers must immediately remediate personal information leaks, distortions, or loss (potential or actual) and notify the designated authorities and the individuals. The notification shall include the following items:

- The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred;
- The remedial measures taken by the handler and measures individuals can adopt to mitigate harm; and
- Contact method of the handler.

Handlers are not required to notify individuals if there was no harm, however, where authorities believe harm may have been created, they may require individuals to be notified. There is no timeframe provided, nor are there references to notifications by entrusted persons.

Handlers are not required to notify individuals if there
was no harm,
however, where authorities believe
harm may have been created,
they may require individuals to be notified.

Data security law

Any data handling taking place within China will also need to meet the requirements of China's Data Security Law (DSL) which entered into force on September 1, 2021. It means that "laws and regulations shall be followed, social public morals and ethics respected, business ethics and professional ethics observed, honesty and trustworthiness [practiced], data security protection obligations fulfilled, and social responsibility assumed, national security and the public interest must not be endangered, and the lawful rights and interests of individuals and organizations must not be harmed." (Article 8 DSL).

Although much guidance is still to be provided for the DSL, "a data security management system for the entire workflow, organizing and conducting data security education and training, and adopting corresponding technical measures and other necessary measures to ensure data security" are all mandatory (Article 27 DSL). The DSL also makes security risk monitoring, and in case of important data, security risk assessments, mandatory.

Handling data transfers

Handlers can transfer personal information, when necessary, due to mergers, separations, dissolution, declaration of bankruptcy, and other such reasons, but must notify individuals of the receiving party's organization or personal name and contact method. The receiving party shall continue to fulfill the personal information handler's duties. When the receiving side changes the original handling purpose or handling method, they shall notify the individual again as provided in this law (Article 22).

Sharing personal information: vendors/processors (entrusted persons)

When handlers share personal information outside the entity, the recipients are considered "entrusted persons" (Article 59) and must only process the information according to PIPL and other applicable laws, safeguard the information, and assist handlers in their obligations under PIPL.

Handlers must notify individuals about any data sharing outside the entity. When this is to another handler (controller to controller), handlers shall provide the organization's name or personal name of the recipient, contact method, purpose for sharing, data categories, and obtain separate consent from the individual (Article 23). Recipients must honor the approved processing — the purposes, methods, categories of data, etc. If recipients change any of this, they must obtain new consent from the individuals.

Vendor contract requirements

Contracts between handlers and entrusted persons must include:

- Purpose of processing (and why shared to this trusted person),
- Time limit,
- Handling method,
- Categories of personal information,
- Protection measures,
- Rights and duties of both sides,
- Supervision,
- Specification that the processing is limited to the activities in the agreement, and
- Handlers must approve subcontractors.

Once the agreement ends, whether voided, canceled, or terminated, the personal information must be destroyed or deleted.

Once the agreement ends, whether voided, canceled, or terminated, the personal information must be
destroyed or deleted.

Cross-border transfers

When handlers “truly need” to transfer personal information outside the borders of China, business, or other requirements, they have to meet the following conditions (Article 38):

- Pass a security assessment organized by the state cybersecurity and information department according to Article 40;
- Undergo personal information protection certification conducted by a specialized body according to provisions by the state;
- Include a contract with the foreign receiving side in accordance with a standard contract formulated by the state cyberspace and information department that notes the agreement of the rights and responsibilities of both sides; and
- Fulfill other conditions provided in laws or administrative regulations or by the state cybersecurity and information department.

At this time, none of these have been identified. The Asia-Pacific Economic Cooperation (APEC) CBPRs were not mentioned and China is not an APEC member. In the first part of PIPL, though, it states that the country “vigorously participates in the formulation of international rules [or norms] for personal information protection, stimulates international exchange and cooperation in the area of personal information protection, and promotes mutual recognition of personal information protection rules [or norms], standards, etc., with other countries, regions, and international organizations” (Article 12). Perhaps the APEC CBPRs will be considered in the future. When China has agreed to treaties or international agreements, any provisions therein would be permitted (Article 38).

Consent from individuals

Handlers transferring data across borders must notify (and obtain separate consent from) individuals about the recipient’s name and/or personal name, contact methods, handling purpose(s), handling methods, and personal information categories, as well as ways or procedures for individuals to exercise their rights under PIPL and other such matters (Article 39).

Critical infrastructure providers and handlers with large quantities of data

As provided above, infrastructure providers and handlers processing large amounts of data are only permitted to use the security assessment provision unless specific law states otherwise (Article 40). Among the items in which guidance is needed is specifying what “large” means.

Government requests

Competent authorities of the People's Republic of China only will handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored in China.

Without the approval of the competent authorities, handlers may not provide personal information stored within China to foreign judicial or law enforcement agencies (Article 41).

Enforcement

> The enforcement measures under PIPL are quite thorough and complex.

The enforcement measures under PIPL are quite thorough and complex. Enforcement options include both civil and criminal penalties (Article 66), and may include:

- Compliance orders;
- Processing bans;
- Confiscation of unlawful income; and
- Fines.

Entities who violate PIPL will be ordered to correct the violation, relinquish income they received which will be deemed unlawful, and suspend those activities which are in violation. If entities refuse to correct their activities, they face an additional fine of up to one million yuan (US$158 million).

For more grave violations, the fine for the entity faces a higher penalty and their business license may be revoked. The maximum penalty for the organization is up to 50 million yuan (US$8 million) or five percent of annual revenue. When violations effect a large number of people, the entity faces lawsuits by the People's Procuratorates (public prosecutors), statutorily designated consumer organizations, and organizations designated by the state cybersecurity and informatization department (Article 70).

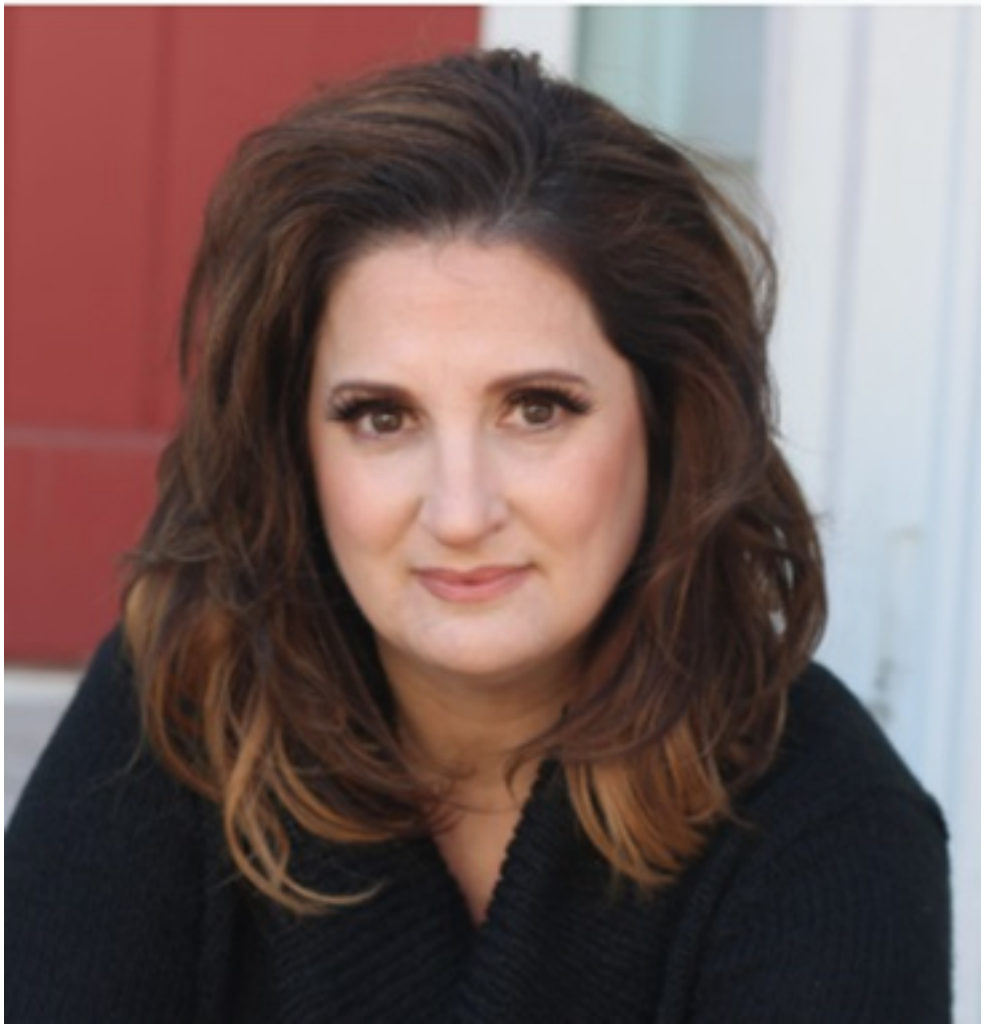
Additionally, persons in charge or directly responsible for the processing operation can receive a personal fine between 10,000 and 100,000 yuan (US$1,578 and US$16,780). The individual sanction would go up to 100,000 and one million yuan for grave violations, but individuals may also be prohibited from “holding positions of director, supervisor, high-level manager, or personal information protection officer for a certain period.” Where applicable, violations will also be reported to individuals’ (and organizations’) credit files and publicized (Article 67).

In addition, where entities reject individuals’ requests to exercise their rights, individuals may file a lawsuit (Article 50). There are also repercussions for government agencies and personnel (Article 68).

Updates

In the time since PIPL was passed, China issued the Draft Measures on Data Cross-Border Security Assessment on October 29, 2021. Prior versions were issued in 2017 and 2019, but this version takes into account both the PIPL and DSL. The draft provides a definition for the “large volume” handlers mentioned above (handling data of one million individuals or more) and circumstances which would require handlers to seek a security assessment by the Cybersecurity Administration of China, such as for “important data” as classified by the government. The draft proposal includes requirements for transferring data on 100,000 individuals or sensitive data on 10,000 people.

K Royal



Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.