WHITEPAPER

TrustArc

China’s Personal Information Protection Law (PIPL)

On August 20, 2021, the National People’s Congress (NPC) of China adopted the Personal Information Protection Law (PIPL) with an effective date of November 1, 2021. It is the first comprehensive data protection law in the People’s Republic of China (China) and leaves little time for compliance preparation before it is enforced.

In this whitepaper, we will discuss:

- Fundamentals of the new law with key definitions
- Enforcement mechanisms and potential fines
- Guidance for compliance by November 1, 2021

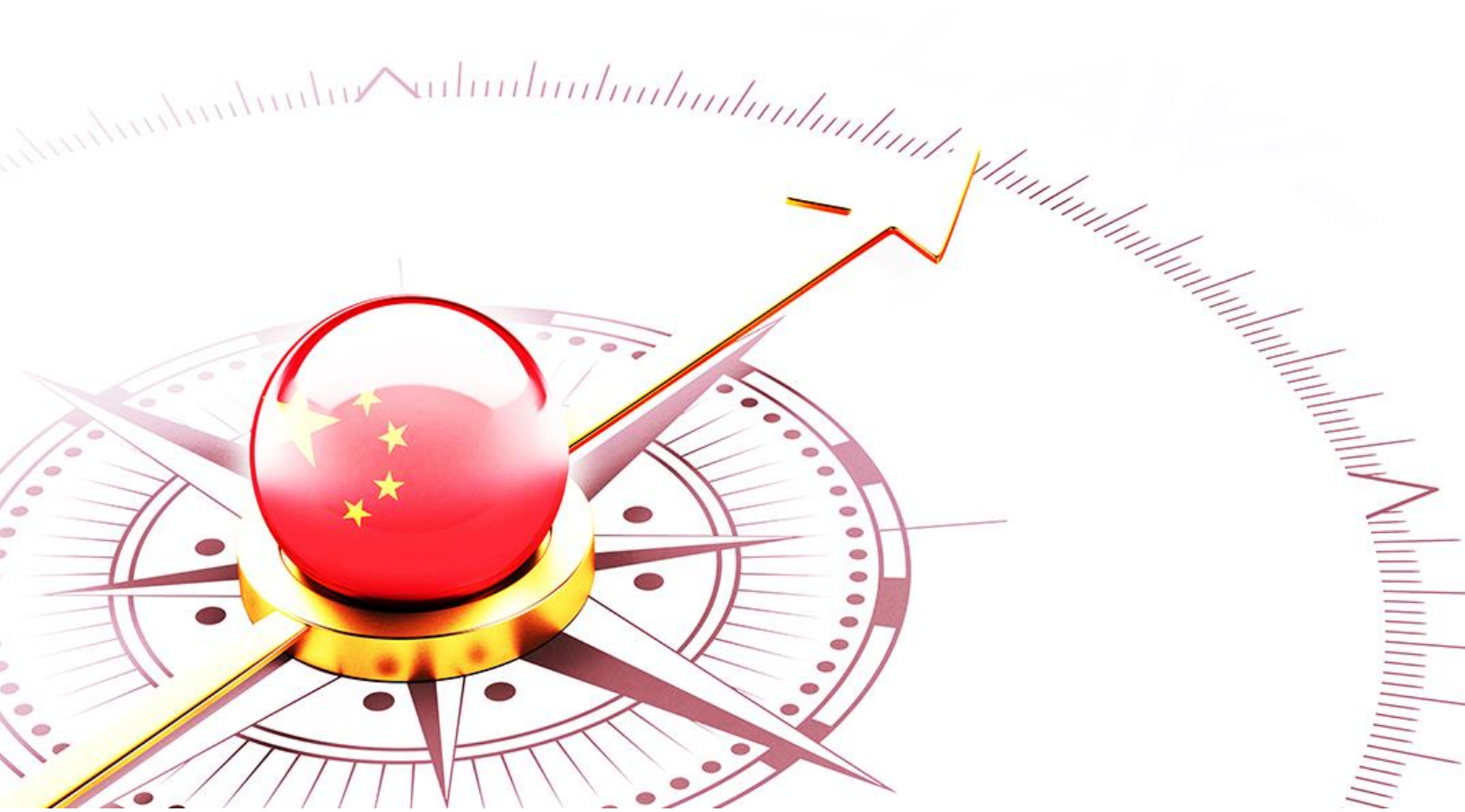
China's Personal Information Protection Law

On August 20, 2021, the National People's Congress (NPC) of China adopted the Personal Information Protection Law (PIPL) with an effective date of November 1, 2021. It is the first comprehensive data protection law in the People's Republic of China (China) and leaves little time for compliance preparation before it is enforced.

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 adopts many of the concepts of the GDPR, such as individual rights, vendor management requirements, and data breach notification.

Core data protection principles like purpose limitation, transparency and data quality are part of the law as well. 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 or 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 - which are only allowed if it is "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 (CAC), which will also be allowed to impose fines. This, and much more, are provided in detail below.



Fundamentals & 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" (Art. 3). Further, processing ("handling" as the PIPL translation refers to it) personal information outside China on individuals in China is also covered if one of three conditions is met:

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

Definitions

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

- 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" (Art. 4).
- Handling is very broad and includes "collection, storage, use, processing, transmission, provision, disclosure, deletion, etc." (Art. 4)
- "Personal information handler" refers to organizations and individuals that, in personal information handling activities, autonomously decide handling purposes (Art. 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" (Art. 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 whitepaper.

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, Handler shall obtain personal consent in accordance with PIPL.

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 (Art. 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 (Art. 29). If there are other laws addressing this information, those laws must be followed.

Some of these obligations are for the notice provisions and others 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 shall obtain the consent of the parent or other guardian of the minor (Art. 31). In addition, they need to develop specialized rules (internal policies and processes) for handling this information.

Principles

Personal information must be handled (processed) under certain principles, and cannot be processed in "misleading, swindling, coercive, or other such ways" (Art. 5). These principles include:

- Legality
- Propriety
- Necessity
- Sincerity
- Transparency (Art. 7)
- Quality & Accuracy (Art. 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 make sure there are no adverse impacts to individuals from inaccurate or incomplete information (Art. 8).

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 harming national security or the public interest (Art. 10).

Personal Information Handling Rules

PIPL provides for specific rules of handling personal information. There are only six (6) circumstances explicitly listed in PIPL, plus allowance for others required by law:

1. Obtaining individuals' consent;
2. Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded contracts;
3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations;
4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;
6. 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
7. 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. (Art. 19).

Individual Rights

Like most privacy laws, PIPL provides individuals with certain rights (Chapter IV), which must be addressed in a timely manner. No timeframe is provided. Except where applicable laws say otherwise, these rights include the following:

- Transparency and notice (Art. 17)
- Know if an entity is processing their personal information (Art. 44)
- Decide if and how their personal information is processed (Art. 44)
- Limit or refuse data processing (Art. 44)
- View and copy (exceptions are provided, mainly if restricted by other laws)(Art. 45)
- Portability (Art. 45)
- Correction and amendment (Art. 46)
- Deletion (Art. 46)
- To know (and have explained) the personal information handling rules, if there are any (Art. 48)
- Non-discrimination for exercising rights (Art. 16)
- Know automated decision-making activities (Art. 24)
- Refuse automated decision-making for significant activities
- Refuse targeted ads done by automation
- Consent to cross-border transfers (Art. 39)

It is noted that portability is truly a porting requirement. PIPL provides in Art. 45 that "[w]here 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 where 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;
- 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 (Art. 50). However, individuals may file a right of action in court to enforce their rights (Art. 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 their death (Art. 50).

Transparency (privacy notice)

Before processing personal information, Handlers shall explicitly provide an accurate (truthful), clear, and understandable privacy notice (Art. 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 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 (Art. 30).
- Cross-border transfers, currently or proposed in future, with separate consent.

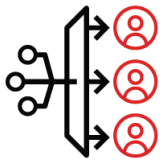
If anything changes, including additional uses for the information or sharing the information outside the entity, Handlers should amend the notice and notify individuals. In many cases, Handlers will need to gain new consent from individuals.

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" (Art. 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 (Art. 16).

Special Processing Activities



Article 73 of PIPL provides four specific definitions, one of which was listed earlier for "personal information handler." The others will be covered here under special processing activities and consent. This section will include consent, automated decision-making, de-identification & 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 (Art. 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 and must agree to such new or different data processing - in advance.

Along with consent, though, comes the revocation of consent (Art. 15). Individuals must be able to revoke consent in a convenient manner. Revocation only impacts future use of the information, not the past use. However, where 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 In order to provide those services or products (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.

Automated Decision-making

"Automated decision-making" refers to the activity of using computer programs to automatically analyze or access personal behaviors, habits, interest, or hobby, or financial, health, credit, or other status, and make decisions [based thereon].

Handlers must be transparent about the decision-making automated process and guarantee the fairness and justice of the result. Handlers are prohibited from engaging in unreasonable differential treatment of individuals in trading conditions, such as with a trade price, etc. (Art. 24)

When the automated decision-making process results in a major influence on the rights and interests of individuals, they have the right to require Handlers to explain the matter, and they have the right to refuse to let Handlers make decisions solely through automated decision-making methods.

Those conducting information push delivery or commercial sales to individuals through automated decision-making methods shall simultaneously provide the option to not target an individual's characteristics, or provide the individual with a convenient method to refuse.

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 the GDPR.

Surveillance

Surveillance has become a global hot topic, partially because it is so widespread, not well-controlled, and benefits from a huge technological market. PIPL prohibits the installation of image collection or personal identity recognition equipment in public venues, unless for public security only, 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.

Cookies

Neither PIPL, nor the DSL contain specific requirements when it comes to the placement of cookies and other trackers. However, they are also not explicitly exempted from the scope of the law. Under the general provisions of the law, it is safe to assume that the placement of cookies and trackers on the equipment of a user that is based in China, constitutes data processing that is covered by PIPL. The handling of cookie and tracker data, would therefore also require a legal basis under Article 13 PIPL and of the provided options, consent seems to fit the case for cookies.

In practice, this means that when people in China visit a website after November 1 that works with cookies and trackers, opt-in consent is required. This consent is similar to the consent requirements under the GDPR and the Brazilian Lei Geral de Proteção de Dados (LGPD) consisting of "a voluntary and explicit statement" of the individual based on full information. Any cookie banner would therefore need to include a privacy notice. Essential cookies can be placed without the individual's consent, based on an exception in Article 16 PIPL, that allows data processing "necessary for the provision of products or services."

Responsibilities of Personal Information Handlers

(Chapter V)

The obligations on each party are not uncommon. 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. In addition, Handlers must 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 (Art. 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 (Art. 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 health care or finance. In addition, 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 (Art. 54).

Joint Handlers

Like many other laws, there is a concept of joint controllership, or in the case of China joint Handlership. Joint handlers shall agree on respective responsibilities between the two of them (or more)(Art. 20), but individuals may enforce their rights against either Handler and they 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" (Art. 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;
- 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 (Art. 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 that 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 (Art. 53).

Impact Assessments

Handlers must perform a documented personal information impact assessment before engaging in the following activities (Art. 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;
- Other personal information handling activities with a major influence on individuals.

Impact assessments must include (Art. 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;
- 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 & Handlers with Large Quantities of Data

These types of Handlers 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;
- 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.

Data Security Law

Any Data Handling taking place within China, will also need to meet the requirements of China's Data Security Law (DSL) that entered into force on September 1, 2021. This means in any case 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" (Art. 8 DSL). Although also for the DSL, a lot of guidance is still to be provided, "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 considered as mandatory (Art. 27 DSL). The DSL furthermore makes security risk monitoring, and in case of important data, security risk assessments, mandatory.

Data Transfers

Data Transfers due to Mergers, etc.

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

Sharing Personal Information - Vendors/Processors (Entrusted Persons)

Where Handlers share personal information outside the entity, the recipients are considered "entrusted persons" (Art. 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. Where this is to another Handler (controller to controller), Handlers shall provide the name or personal name of the recipient, contact method, purpose for sharing, data categories, and obtain separate consent from the individual (Art. 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
- Limited to the activities in the agreement
- Handlers must approve subcontractors

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

Cross-Border Transfers

(Chapter 3)

Where Handlers "truly need" to Transfer personal information outside the borders of China or business or other requirements, they have to meet the following conditions (Art. 38):

- Passing a security assessment organized by the State cybersecurity and information Department according to Article 40;
- Undergoing personal information protection certification conducted by a specialized body according to Provisions by the State;
- Including a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and information Department, agreeing upon the rights and responsibilities of both sides;
- 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 APEC CBPRs were not mentioned, and China is not currently a member of the Asia-Pacific Economic Cooperation. In the first part of PIPL, though, it is stated 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" (Art. 12). Perhaps the APEC CBPRs is still up for consideration in the future. When China has agreed to treaties or international agreements, any provisions therein would be permitted (Art. 38).

Consent from Individuals. Handlers transferring data across borders must notify (and obtain separate consent from) individuals about the recipient's name / 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 (Art. 39).

Critical Infrastructure Providers & Handlers with Large Quantities of Data, as provided above, are only permitted to use the security assessment provision unless specific law states otherwise (Art. 40).

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 (Art. 41).

Reciprocating Actions

China clearly provides for the ability to reciprocate in kind.

- Where foreign organizations or individuals engage in personal information handling acts violating personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cybersecurity and informatization department may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc. (Art. 42).
- Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt reciprocal measures against said country or region on the basis of actual circumstances (Art. 43).

Enforcement

The enforcement measures under PIPL are quite thorough and complex. Enforcement options include both civil and criminal penalties (Art. 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 the unlawful income, and suspend those activities which are in violation. If entities refuse to correct their activities, they face an additional fine of up to 1 million Yuan.

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 (~$7,7 million) or 5% of annual revenue. Where violations impact 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 (Art. 70).

Additionally, persons in charge or directly responsible for the processing operation can receive a personal fine between 10,000 and 100,000 Yuan. The individual sanction would go up to 100,000 and 1 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 (Art. 67).

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

Government Duties and Responsibilities
(Chapter VI)

This chapter specifically addresses the duties and responsibilities of the designated agencies and departments.

Responsibilities
The State cybersecurity and informatization department is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work.

Relevant State Council departments are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations (Art. 60).

County-level and higher people's governments' relevant departments' personal information protection, supervision, and management duties and responsibilities are determined according to relevant State provisions.

"Departments fulfilling personal information protection duties and responsibilities" refers to all of the above. Below, we will simplify the reference with "Departments."

Departments are responsible for (Art. 61):

- Conducting personal information protection propaganda and education, and guiding and supervising personal information handlers' conduct of personal information protection work;
- Accepting and handling personal information protection-related complaints and reports;
- Organizing evaluation of the personal information protection situation such as procedures used, and publishing the evaluation results.
- Investigating and dealing with unlawful personal information handling activities;
- Other duties and responsibilities provided in laws or administrative regulations.

The State cybersecurity and informatization department coordinates overall the following personal information protection work by the relevant departments (Art. 62):

- Formulate concrete personal information protection rules and standards;
- Formulate specialized personal information protection rules and standards for small-scale personal information handlers and new technologies and new applications for handling sensitive personal information, facial recognition, artificial intelligence, etc.;
- Support the research, development, and broad adoption of secure and convenient electronic identity authentication technology, and promote the construction of public online identity authentication services;
- Advance the construction of service systems to socialize personal information protection, and support relevant organizations to launch personal information protection evaluation and certification services;
- Perfect personal information protection complaint and reporting work mechanisms.

When Departments fulfill personal information protection duties and responsibilities, they may adopt the following measures (Art. 63):

- Interviewing relevant concerned parties, and investigating circumstances related to personal information handling activities;
- Consulting and reproducing a concerned party's contracts, records, and receipts as well as other relevant material related to personal information handling activities;
- Conducting on-site inspections, and conducting investigations of suspected unlawful personal information handling activities;
- Inspecting equipment and articles relevant to personal information handling activities; and when there is evidence the equipment or articles are used to engage in illegal personal information handling activities, after reporting to their department's main person responsible in writing and receiving approval, they may seal or confiscate them.

Where Departments fulfill their duties and responsibilities according to the law, concerned parties shall provide assistance and cooperation, and they may not obstruct or impede them.

When Risks are Discovered

Where Departments discover relatively large risks exist in handling activities or security incidents occur, they may conduct a talk with the Handler's legal representative or main person responsible according to regulatory powers and procedures, or require Handlers to entrust specialized institutions to conduct compliance audits of their handling activities. Handlers shall adopt measures according to requirements to correct the matter and eliminate the vulnerability (Art. 64).

Where Departments discover in the course of their duties discover unlawful handling of personal information that is suspected of constituting a crime, they shall promptly transfer the matter to public security authorities for processing according to the law (Art. 65).

File Complaints

Any organization or individual has the right to file a complaint or report about unlawful personal information handling activities with Departments. Departments receiving complaints or reports shall process them promptly and according to the law, and notify the complaining or reporting person of the handling outcome (Art. 65).

Contact

Departments shall publish contact methods to accept complaints and reports.

How to Comply in Less Than 60 Days with TrustArc

With a short deadline, the only way to build demonstrable evidence and reporting that shows how your business complies is to use what you already have in place. You can begin by compiling the evidence that shows your foundational privacy program elements and also PIPL-specific work as it is developed.

In PrivacyCentral, we map the overlap of privacy laws, including PIPL, so you only have to upload evidence once. This means, if you upload your existing GDPR work such as policies and procedures today, we'll automatically apply the documentation and evidence to PIPL, and any other new laws.

PrivacyCentral will highlight the gap between GDPR and PIPL, so you'll need to only action the delta between the two laws.

Know where you stand. Know what to do.

BOOK A DEMO TODAY