Achieving PIPL Compliance With Avature

What You Need to Know About China's Personal Information Protection Law (PIPL)

The Personal Information Protection Law (PIPL) is China's most comprehensive law in the personal information protection field so far. Based on the People's Republic of China's (PRC) Constitution, the PIPL aims to "protect the personal information rights and interests of individuals," "regulate personal information processing activities," and "promote a reasonable use of personal information" (Article 1).

Echoing the European Union's General Data Protection Regulation (GDPR), the PIPL is applicable to organizations and individuals who process personal information (PI) within the territory of China or outside its territory when offering products or services to individuals in the PRC or analyzing or assessing the behavior of individuals in the PRC. The PIPL creates a legal framework for processing of PI from the perspectives of national security and digital sovereignty that are consistent with the PRC's current policy priorities and also emphasizes the protection of the rights of individuals against abuse, aligning the PRC with the growing international consensus around the protection of the privacy of individuals.

The PIPL is defined by strong data subject rights, stringent requirements on data sharing and data transfers (including data localization provisions) and serious corrective actions for those organizations that fail to adhere to the legal regime, including penalties and fines (up to 50 million RMB or five percent of an organization's annual revenue), confiscation of illegal income and suspension of services. The PIPL comes into effect on November 1, 2021.

In order to be in compliance, Avature customers will need to:

- Be familiar with the PIPL guiding principles and specific requirements.
- Establish business processes that are designed to support those principles and requirements.
- Process personal information of candidates and employees in a legally compliant manner and ensure their data processing activities provide adequate technical controls.

Impacted Parties

Generally, the PIPL oversees two groups that either have rights or obligations in respect of the PI. When working with Avature, these are:

- Individuals (i.e., candidate/employees)
- Personal information (PI) processor (i.e., customer) and entrusted party (i.e., Avature)

Under the PIPL, your candidates and employees are the individuals, to whom the PIPL grants rights. It is their PI that is processed when they are considered for a position, kept in a talent pool, or managed as an employee. Your organization will act as a PI processor, responsible for independently determining the purpose and method of processing PI , the type of information to be processed and the applicable retention period.

Your organization is also responsible for supervising any processing activities entrusted to Avature as a third-party processor.

Article 21 of the PIPL refers to the conditions applicable to a PI processor who wishes to entrust another party the handling PI . Note that PI is defined as any type of information relating to identified or identifiable natural persons, recorded by electronic or other means (e.g., name, address, mobile phone number, etc.). In addition, Article 59 of PIPL specifies the requirements applicable to the entrusted party when handling PI on behalf of PI processor, including (i) taking necessary security measures for processing activities, and (ii) providing assistance to PI processor for fulfilling their obligations under PIPL.

Guiding Principles

The PIPL establishes seven principles for PI processing that organizations are required to comply with when processing PI.

Legality: PI shall be processed in accordance with the principles of lawfulness, legitimacy, necessity and good faith, and not in any manner that is misleading, fraudulent or coercive.

Explicit Purpose: Processing of PI shall be done for a specified and reasonable purpose (i.e., one that is directly relevant to the PI processing), and in a way that has the least impact on personal rights and interests.

Data Minimization: Collection of PI shall be limited to the minimum scope necessary for achieving the purpose of processing and shall not be excessive.

Transparency: PI shall be processed in accordance with the principles of openness and transparency, disclosed with the rules of processing of PI and the purpose, method and scope of processing expressly stated.

Accuracy: The quality of PI shall be ensured to avoid adverse effects on personal rights and interests caused by inaccurate and incomplete PI.

Accountability and Security: PI processors shall be responsible for their processing activities and take necessary measures to ensure the security of the PI processed.

Storage Limitation: The retention period of PI shall be the minimum period necessary for achieving the purpose of processing unless any law or regulations stipulate otherwise.

Cross-Border Provision of Personal Information

In general, the PIPL mandates that PI be processed within the territory of the PRC. Where it is necessary to transfer PI to entities outside of the PRC, the PI processor is required to:

- Provide individuals with certain specific information about the transfers and obtaining separate consent (Article 39).
- Fulfill one or more of the required conditions set out in the PIPL (security assessment, certification by a professional institution, standard contract, other conditions prescribed by law, administrative regulations or the Cyberspace Administration of China (CAC)). In any case, PI Processors are required to ensure that the overseas recipients can provide the same level of protection as required under the PIPL (Article 38).
- Carry out a personal information protection impact assessment (Article 55).

If the processing entity is a Critical Information Infrastructure (CII) operator or entity processing a large amount of PI, PI is required to be stored locally. If it is indeed necessary for it to transfer such PI overseas, it shall pass a security assessment administered by the Cyberspace Administration of China (CAC) (Article 40). Note that the PIPL requires the retention of data processing records and the personal information protection impact assessment for at least three years when transferred (Article 56).

Obligations of PI Processors

Under the PIPL, the "processing" of PI refers to the collection, storage, use, processing, transmission, provision, publication and erasure of PI (including information recorded by electronic or other means and processed automatically). The PIPL establishes the following main obligations for PI processors to prevent PI from any unauthorized access, leakage, tampering or loss:

i. Providing required notices or disclosure of processing activities to individuals;

ii. obtaining valid legal grounds for processing activities, including consent by individuals;

iii. implementing the necessary security measures to protect PI from any unauthorized access, leakage, tampering or loss;

iv. if applicable, complying with the PRC's data transfer provisions, including adopting appropriate mechanisms legalizing such transfers;

v. if applicable, appointing a personal information protection officer;

vi. conduct internal compliance reviews on a regular basis;

vii. if applicable, conduct personal information protection impact assessment reports.

A PI processor can contract the processing of PI to a third-party (i.e., entrusted party). Article 21 and Article 59 governs the rights and responsibilities of each party.

The PI processor and the entrusted party will need to agree on the purpose, duration and method of the processing, the type of information to be processed, the protection measures to be applied and the rights and obligations of both parties.

The entrusted party is limited to the agreed upon scope of the processing (i.e., purpose and method), and if the contract is invalidated or terminated, must return the PI to the PI processor or delete it. The entrusted party shall also take necessary security measures for processing activities, and assist PI processor in fulfilling their obligations under PIPL.

HR Challenges and Opportunities

Recruiting and talent management programs, which depend on collecting and using personal information, face one of the biggest challenges with respect to PIPL compliance. The PIPL will require a balancing act between hiring the best candidates and the protection of personal information. Avature customers operating out of the PRC but collecting personal information of PRC residents should expect an increase in process complexity and run the risk of extremely high fines for non-compliance.

And yet, strict compliance with the PIPL will also provide Avature customers with a significant competitive advantage as candidates will be more willing to share data with your organization. With Avature as your trusted data processor (Entrusted Party), you can expect to:

- Clean up your recruiting system to identify strong candidates and reduce the need to acquire new talent.
- Update candidate information.
- Rediscover talent in your database.
- Improve engagement by periodically checking in with candidates in your talent pools.

How Avature Can Help as an Entrusted Party

From the GDPR to California's Consumer Privacy Act, Avature has been helping customers comply with similar privacy laws for years.

Our customers - which include large and small enterprises, all the major global consulting companies, many of the largest banks and manufacturers in the US that do business in the PRC - have developed competitive recruiting programs that operate effectively throughout the world and meet each jurisdiction's data regulations.

Specifically, to the PIPL, we also have extensive expertise and experience processing data in the PRC. Avature offers data localisation capabilities in the PRC and we take reasonable precautions to protect PI in the data center from loss, misuse and unauthorized access, disclosure, alteration and destruction. In addition, in case it is needed to achieve compliance, Avature expects to be able to enter into the China Cyberspace Administration's model contract for cross-border data transfers once it is made available.

Leveraging our fundamental focus on configuration, we have invested in technical functionality specifically designed to support privacy laws. Our system is highly adaptable, and you can determine how to process data in a manner that is legally compliant.[1]
When compliance regulations change, our technology can keep pace.

We have also assisted customers in their response to government inquiries relating to individual citizens' privacy complaints and supported customers in their successful resolution of complaints. Our legal team knows how to draft, review and execute amendments to existing data protection agreements.

Features

Specific to the PIPL, our solutions offer different features to help you achieve compliance.

Consent forms to manage and keep track of individuals' consent with timestamps.

Customizable opt-in/out or double opt-in workflows that automate the consent process and regularly re-evaluate candidate consent.

Automated purging or deletion of data at intervals determined by you.

Encryption that keeps confidential data accessible and editable on a need-to-know basis.

Configurable security settings for your users in accordance with your security needs.

Full audit journal to trace interactions with candidates, including consents, updates and changes.

Unsubscribe links in emails sent through Avature so candidates can choose to opt out.

Data export reports to provide candidates with copies of their data.

Support and Security Measures

Our main responsibilities as an entrusted party under the PIPL are to take the necessary measures to ensure the security of PI and to assist the PI processor in fulfilling its

[1] While Avature offers functionalities to support compliant processes, we are not a law firm and do not provide legal advice. We have, however, worked directly with the legal departments of major organizations and their recruiting and talent management teams to implement compliant programs. Avature's consultants have supported the implementation of many programs for customers operating in China, following their requirements in accordance with Chinese privacy laws. We strongly recommend you consult with your legal counsel to decide upon compliance processes.

obligations. To do so, we implement a number of technical and organizational security measures behind the user interface, including:

- Firewall, encryption and other technologies to protect the information.
- Separation of processing for different customers and their different purposes.
- Role segregation so that only Avature employees who need to access sensitive data are able to view it.

The operations, policies and controls at Avature are audited regularly to ensure that our solutions meet and exceed all requirements expected of a world-class technology service provider.

Avature's standard of excellence is supported by our commitment to maintaining our ISO, SOC 1 and SOC 2 certifications. Avature's cloud is operated out of carrier-neutral colocation data centers in the PRC, and we offer our customers a full-service and experienced team of local experts.

With PIPL coming into effect, if your legal counsel advises you to reconfigure your instance, please contact your sales representative and our consultants will support any reconfiguration according to your instructions. For more information, contact your sales representative or email **sales@avature.net.**

"At Avature we are used to working with large, complex, multinational businesses so this is not the first time we have assisted our customers in complying with new privacy regulations. As we inevitably see more regulation changes across different markets, I am confident that our customizable platform will enable customers to adapt to these changes while ensuring their recruiting programs remain as competitive as ever."

Manuel Sevilla
Data Privacy Officer

obligations. To do so, we implement a number of technical and organizational security measures behind the user interface, including:

- Firewall, encryption and other technologies to protect the information.
- Separation of processing for different customers and their different purposes.
- Role segregation so that only Avature employees who need to access sensitive data are able to view it.

The operations, policies and controls at Avature are audited regularly to ensure that our solutions meet and exceed all requirements expected of a world-class technology service provider.

Avature's standard of excellence is supported by our commitment to maintaining our ISO, SOC 1 and SOC 2 certifications. Avature's cloud is operated out of carrier-neutral colocation data centers in the PRC, and we offer our customers a full-service and experienced team of local experts.

With PIPL coming into effect, if your legal counsel advises you to reconfigure your instance, please contact your sales representative and our consultants will support any reconfiguration according to your instructions. For more information, contact your sales representative or email **sales@avature.net.**

"At Avature we are used to working with large, complex, multinational businesses so this is not the first time we have assisted our customers in complying with new privacy regulations. As we inevitably see more regulation changes across different markets, I am confident that our customizable platform will enable customers to adapt to these changes while ensuring their recruiting programs remain as competitive as ever."

Manuel Sevilla
Data Privacy Officer

Appendix

GDPR vs. PIPL

While the PIPL is similar to the GDPR in many ways, it imposes a number of substantive obligations that differ from the GDPR, and there are a number of obligations in the GDPR that are not included in the PIPL. We highlight these differences below.

Key Terms

"Personal information" and "processing of personal information" are defined similarly under both the PIPL and the GDPR. Sensitive personal information is referred to under the PIPL as, "personal information that, once leaked or illegally used, may easily infringe the dignity of a natural person or cause harm to personal safety and property security, such as biometric identification information, religious beliefs, specially-designated status, medical health information, financial accounts, information on individuals' whereabouts, as well as personal information of minors under the age of 14." (Article 28).
Note that as opposed to the GDPR's closed list of items that qualify as sensitive information, the PIPL is an open list that is open to interpretation.

Under the PIPL, anonymized information is not deemed to be PI. Here, "anonymization" refers to the process by which PI can no longer be used to identify specific natural persons, and such anonymized PI cannot be restored to PI in any way (Articles 4 & 73).

The PIPL uses the term "entrusted person" to refer to the "data processor" as defined by the GDPR. The "data controller" concept defined under the GDPR is referred to as "PI processor" under the PIPL and refers to an "organization or individual that independently determines the purposes and means for processing of PI" (Article 73).

Territorial Scope

Similar to the GDPR, the PIPL extends its territorial scope to the processing of PI conducted outside of the PRC under certain circumstances (Article 3). Mirroring the GDPR's requirement of the appointment of an "EU representative" for offshore controllers, the PIPL also requires offshore PI Processors subject to the PIPL to establish a "special agency" or appoint a "designated representative" in the PRC for PI protection purposes (Article 53).

Lawful Basis

As with the GDPR, the PIPL requires organizations to have a lawful basis to process PI (Article 13). However, the PIPL does not provide "legitimate interests" as a lawful basis for processing, as found in the GDPR.

With respect to "consent," the definition under Articles 14 and 15 of the PIPL aligns with the consent requirements of the GDPR (i.e., it must be informed, freely given, demonstrated by a clear action of the individual, and may later be withdrawn).

Note that the PIPL requires a separate consent for certain processing activities, namely if a PI processor (i) shares PI with other PI processor; (ii) publicly discloses personal information; (iii) processes sensitive PI; or (iv) transfers PI overseas (Articles 23, 25, 29 and 39).

Data Subject Rights

Under both the GDPR and the PIPL, individuals have certain rights that organizations (i.e., "data controllers" or "PI processors") must uphold. A data subject access request is one way an individual can submit a request to exercise one or more of those rights. Under the GDPR, an organization generally has 30 days to respond to such requests, while under the PIPL, organizations have 15 days to respond. Although PI rights provided for under the PIPL are generally similar to those under the GDPR, it remains uncertain how such rights under the PIPL might be interpreted and enforced in practice:

Rights under the GDPR	Rights under the PIPL
Right to access	✓
Right to correction/rectification	✓
Right to erasure	✓
Right to object to and restrict the processing of an individual's data	✓
Right to data portability	(under certain conditions)
Right not to be subject to automated decision-making	✓
Right to withdraw consent	✓
Right to lodge a complaint with the regulator	✓

One important difference to note is that whereas under the GDPR, every data subject is expressly granted the right to lodge a complaint with a supervisory authority in case of infringement of his or her rights, under the PIPL individuals have the right to bring lawsuits against PI Processors if they reject the individuals' requests to exercise their rights (Article 50). However, any organization or individual can lodge a complaint with the supervisory authority that is in charge of personal information protection in case of any unlawful activities conducted by PI processor (Article 65).

Personal information protection impact assessment

The PIPL requires PI Processors to carry out prior a personal information protection impact assessments and retain the processing records for at least three years for the following processing activities (Articles 55 and 56):

- Processing of sensitive PI.
- Processing of PI for automated decision-making.
- Contracting an Entrusted Party to process PI, sharing PI with other PI processor or publicly disclosing PI.
- Providing PI to an overseas recipient.
- Other PI processing activities that may have significant impacts on the rights and interests of individuals.

Although a similar obligation to perform a prior PI protection impact assessment is contained under the GDPR (data protection impact assessments or DPIA), the processing activities that will trigger such requirement are different. In addition, under the PIPL, there is no obligation to consult a regulator in the event the result of the assessment is that certain residual risks identified cannot be remediated.

Contact Us to Learn More

For more information about Achieving PIPL Compliance,
please contact your Avature representative or visit our website

www.avature.net

Avature