CLIENT ALERTS & INSIGHTS

China Passes the Personal Information Protection Law

SEPTEMBER 21, 2021

Authors: Ryan T. Sulkin

The law will take effect on November 1, 2021 giving companies under two months to ensure their privacy policies and systems comply.

On August 20, the Standing Committee of the 13th National People's Congress of China passed a sweeping privacy law meant to ensure heightened security of Personal Information ("**PI**") and regulates data standards. Broadly, the law tracks with other omnibus privacy protection laws, such as the General Data Protection Regulation ("**GDPR**") in the European Union.

The Personal Information Protection Law ("**PIPL**") is similar to the GDPR in scope and in the principles it lays out. For example, both laws require lawful processing purposes, notice and consent, data minimization, and grant individual privacy rights. The PIPL also closes gaps in China's data protection regulatory scheme, giving a definition to PI and further defining Sensitive Personal Information ("**SPI**").

While the PIPL is comprehensive and more specific than previous China data protection laws, the law still references "other regulations" that are not published yet and leaves in place vague language to give China flexibility in how they will enforce the new law. Below are key provisions and requirements.

Scope

The PIPL applies to processing of PI that occurs both inside and outside of China. A processor that operates outside of China falls under the PIPL if they process PI (1) for the purpose of providing products or services to persons in China; or (2) to analyze and evaluate the behavior of persons in China. This new law is similar to the GDPR in scope and applicability.

PI is defined as information related to an identified or identifiable person. The definition applies to any PI whether recorded electronically or otherwise. Additionally, PI processing is defined broadly to include any handling of PI.

SPI is PI that, if breached or accessed, could easily infringe an individual's dignity, or harm a person or their property. SPI includes biometric information, religious beliefs, medical health information, financial accounts, geo-location data, and PI of minors under the age of 14. The definition also includes an undefined "specific identities" category of SPI. Regardless, separate notice and consent requirements apply to SPI as explained below.

Lawful Basis

Like other overarching privacy regulations, the PIPL requires a lawful basis for collecting and processing PI-the largest basis being personal consent.

Outside of consent, lawful collection and processing of PI can occur if it is (1) necessary for performance under a contract with the person; (2) necessary to implement a human resources management system in accordance with labor laws and regulations; (3) necessary to perform under statutory or legal duties; (4) necessary to protect the life, health, or property of a person; (5) necessary to respond to a public health emergency; (6) to carry out news, public opinion, or other public interest initiatives; (7) using PI, within a reasonable scope, that an individual already disclosed; and (8) any other circumstances stipulated by laws or regulations.

Notice and Consent Requirements

To obtain consent, the PIPL lays out specific privacy notice requirements. Notices must be displayed in a conspicuous manner and written in easy to understand language.

A PIPL compliant privacy notice must include (1) the name and contact information of the PI processor; (2) a specific processing purpose; (3) the method of processing; (4) the types of PI collected and processed; (5) the retention period of that PI; (6) methods and procedures that consumers may use to exercise rights granted under PIPL; and (7) anything else required by applicable law.

Like other omnibus privacy laws and regulations, the PIPL allows an exception for emergencies, so long as notice is promptly given after the emergency subsides.

A PI processor is also barred from disclosing any PI about an individual to a third party unless that individual's consent is obtained, or where disclosure is required by other laws and regulations.

Data Localization and Cross-Border Transfer

Under other regulations and laws in China, information pertaining to state secrets and important data (defined as anything related to national security, public health, social stability, etc.) are already largely prohibited from cross-border transfer.

While the PIPL is structured in a way to favor data localization, cross-border transfer is allowed if a processor either (1) passes a Cyberspace Administration of China ("CAC") security assessment; (2) receives certification from CAC-certified professional organization; (3) enters into standard contractual clauses to ensure proper flow down of PI protection requirements; or (4) complies with other regulations or requirements imposed by the CAC.

Because it is not clear exactly how the CAC will administer the first two options, standard contractual clauses will likely be the most common cross-board transfer mechanism. Those standard contractual clauses are forthcoming. Additionally, the law requires a PI processor to conduct regular due diligence to ensure any oversea recipients of PI are complying with the standard contractual clauses.

Regardless of the mechanism, a PI processor must give an individual separate notice and receive separate consent prior to initiating a cross-border transfer. That notice must include the (1) name of the overseas recipient; (2) contact information; (3) processing purpose and method; (4) type of PI being transferred; and (5) the procedures through which a person can exercise their rights.

Further. certain Critical Information Infrastructure ("**CII**

") PI processors that process a large volume of PI are prohibited from cross-border transfer unless it is necessary, and the entity passes CAC-certified security assessment.

Sensitive Personal Information

The collection and processing of SPI requires separate notice and consent, and can only occur if the SPI is needed for a specific purpose, there is sufficient necessity, and the processor has strict protection measures in place. The additional notice requirements include informing the individual of (1) the specific purpose and necessity for collecting and processing their SPI; and (2) the impacts it has on their personal rights and interests.

If a processor knows, or reasonably should know, that they are processing PI of a child under the age of 14, consent of a parent or guardian is required. A processor who processes PI of a child under the age of 14 is also required to adopt specific rules and procedures for handling this category of SPI.

Consumer Rights

The PIPL also grants individuals several rights on par with the GDPR and other omnibus privacy laws or regulations. Individual rights under PIPL include a right to (1) know (notice); (2) access; (3) correction; (4) deletion; and (5) transfer (portability).

In tandem with the right to deletion, and like the GDPR, the PIPL principle of data minimization requires that PI be collected and retained only as long as necessary to achieve the stated processing purpose.

Further, under the right to deletion, processors have a proactive obligation-although not necessarily rising to the level of a legal requirement-to delete PI when either (1) the processing purpose no longer exists; (2) the period of retention expires; (3) the processor is no longer providing services; (4) an individual withdraws consent; or (5) the PI was processed illegally. At a minimum, a processor must delete such information upon request by the individual.

Security System and Policy

Under the new law, a proper security and PI protection system is required. What that system and policy entails depends on balancing factors such as the type of PI being processed, the method of processing, and any potential risks or hazards. Characteristics of a compliant system and policy would include (1) internal systems and procedures; (2) management of PI by classification under China's Data Security Law framework; (3) technical measures like encryption and de-identification; (4) reasonable employment and training practices; and (5) creation and maintenance of emergency plans for breaches.

At a minimum the system and policy must be designed to prevent unauthorized access, breach, alteration, or loss of PI. If a breach does occur, the PIPL requires notice to be sent to the CAC with information that includes the type and cause of breach, the PI affected and possible harm, remedial measures being taken, and contact information.

Additionally, the PIPL requires any PI processor located outside of China to establish an office, or designate a representative, within China to be responsible for PI protection.

Security impact assessments are also required under PIPL where a processor is processing SPI, using PI in automated decision-making, disclosing PI, or transferring PI outside of China. Those assessments should include: (1) whether the stated processing purposes are legitimate; (2) any impacts on individual rights or security risks; and (3) whether the security systems and policies are proportional.

Large internet service providers have more requirements to meet. Those include (1) establishing and completing compliance systems; (2) creating an independent oversight body; (3) abiding by principles of openness, fairness, and justice; (4) stopping any services that violate laws designed to protect PI; and (5) regularly releasing PI protection reports.

As PIPL compliance comes into effect and PIPL obligations continue to be amended and further interpreted, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in complying with legal obligations. We are available to assist you with any compliance efforts.

For more information, please contact a member of Benesch's Data Protection Team.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.