Cristina Blanton
Chief Privacy & Data Protection Officer
Office of Systemwide Compliance

The University of Texas System

China's Personal Information Protection Law (PIPL)- 2021

When is it effective?

November 1, 2021. This law expands China's current law, which focuses on the protection of Chinese citizens' personally identifying information (PII). The mission behind the law is to "protect the rights and interests of individuals," "regulate personal information processing activities," and "facilitate reasonable use of personal information" (Article 1). PIPL will not apply to residents in Hong Kong, Taiwan, or Macao.

What is the law about?

PIPL is rooted in the same principles and procedures as the recent General Data Protection Regulation (GDPR). PIPL is aimed at enhancing privacy rights for natural persons within the territory of the People's Republic of China. This law will include many of the same requirements as well, such as breach notification reporting, appointment of a data protection officer, extensive data owner rights including the right to erasure, and others.

PIPL will define PII in a similar manner to GDPR and require some of the same "processing" requirements mandated by GDPR. However, PIPL expands oversight and obligations on processors of data to include the entire life cycle of data from its collection to deletion, whereas GDPR oversight is limited to data while in the use and transmission of a processor.

> Note: For UT institutions, "processor" or "processing" is akin to sharing of data with a third party performing contracted services, i.e., sharing FERPA data with the online student enrollment platform or sharing ePHI with EY for audit purposes.

Personal Information is defined as "all kinds of information relating to identified or identifiable natural persons recorded by electronic or other form, excluding anonymized information."

Processing of personal information includes, among other things, the collection, storage, use, refining, transmission, provision, public disclosure and deletion of personal information.

Sensitive Personal Information is defined 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).

Personal Information Processing Entity: "organization or individual that independently determines the purposes and means for processing of personal information", which are called "data controllers" under GDPR.

Entrusted Party: a data processor as defined by GDPR.

Does PIPL apply to U.S. public entities, e.g., UT institutions?

Yes, and to overseas entities that process or control the PII of Chinese residents. This territorial reach of China's law to the U.S. is the concept of extra-territoriality, introduced to us in GDPR.

PIPL will be triggered for UT institutions when the following criteria is met:

> processing of personal information (of Chinese residents) conducted outside of China, provided that the purpose of the processing is: (i) to provide products or services to individuals in China, (ii) to "analyze" or "assess" the behavior of individuals in China, or (iii) for other purposes to be specified by laws and regulations (Article 3).

While PIPL will commonly affect many tech companies in the United States, it is less likely to routinely impact UT institutions. Each institution will be required to make a case-by-case determination as to PIPL's applicability based on the following:

1. Origination of data
    a. Will PII data be gathered from residents of China? Chinese nationals on student visas will fall into this category. PIPL may need to be considered if an institution must share data about a Chinese student with the student's country of origin. If an American institution works with a Chinese academic institution, it may receive PIPL updates in the next Foreign Affiliation Agreement (FAA).

    b. Are services or products being marketed or provided to residents of China? One-way communications do not fall under PIPL, e.g., announcement of enrollment opportunities, newsletters, and website content accessed by a Chinese resident. Interactive solicitations or marketing, however, may trigger PIPL.

    c. Is the institution conducting research using data from a Chinese organization? If data will be de-identified/anonymized, PIPL is unlikely to apply. If data is identified, a research contract may include components of PIPL compliance. See cross-border transfers below.

2. Identify the Data Controller/Processor
    a. Is the vendor based in China or a global organization with global privacy obligations? PIPL may apply only to the vendor, but the vendor may attempt to pass on certain PIPL obligations to the UT institution. Accordingly, the institution should review the proposed contract terms carefully.

    b. Is the UT institution conducting a joint research project with a Chinese entity? If so, PIPL provisions may need to be considered and compliance responsibilities shared between the parties as co-personal information processing entities.

c. Does the engagement include a cross-border transfer of data from Chinese residents? This includes engagement with a Chinese vendor housing or controlling data gathered from Chinese residents and engaged to transfer personal information to a third party (UT institution) overseas. Institutions may be asked to share responsibilities PIPL puts on the vendor, so they should review the proposed terms carefully to ensure that unnecessary responsibilities are not undertaken. Institutions should also note that they may be required to share certain general security measures with the vendor to ensure secure transfer and storage of PIPL data. This information should not include proprietary or confidential security information.

What are the obligations of an institution if PIPL applies?

Similar to GDPR, when PIPL applies to an engagement, these key components must be present within the contract or at the first point of data contact:

1. Clear and unambiguous **consent** provided to and gathered by the individual, if data is to be used in any manner beyond that provided by PIPL (or if consent is required by other law).

2. **Privacy statement and policy** provided to individuals explaining the purpose for gathering the data, any sharing or use of the data, the privacy officer to contact for explanation of data usage, the data retention period, and other matters required by other law. This is required regardless of consent.

3. **No consent** needed if data is gathered and processed for:
    a. The conclusion and performance of a contract in which the individual is a party, or if the data is necessary for human resource management in accordance with the applicable labor rules and regulations and any collective bargaining obligations;
    b. Performing legal duties or legal obligations;
    c. Responding to public health emergencies, or protecting natural persons' life, health, and property safety under emergency circumstances;
    d. Processing, within a reasonable scope, personal information for conducting news reports, public opinion supervision, and other acts in the public interest;
    e. Processing, within a reasonable scope and in accordance with PIPL, of personal information that has been made public by data subjects or through other lawful means.

Please contact your legal officer for any questions specific to the application of PIPL at your campus. For general PIPL questions, please contact, Cristina Blanton- Chief Privacy Officer, cblanton@utsystem.edu.