Additional Requirements for Research Subject to China's Personal Information Protection Law (PIPL)

Effective November 2021, China's Personal Information Protection Law (PIPL) sets strict regulations on the collection, storage, use, and transfer of personal information of Chinese citizens.

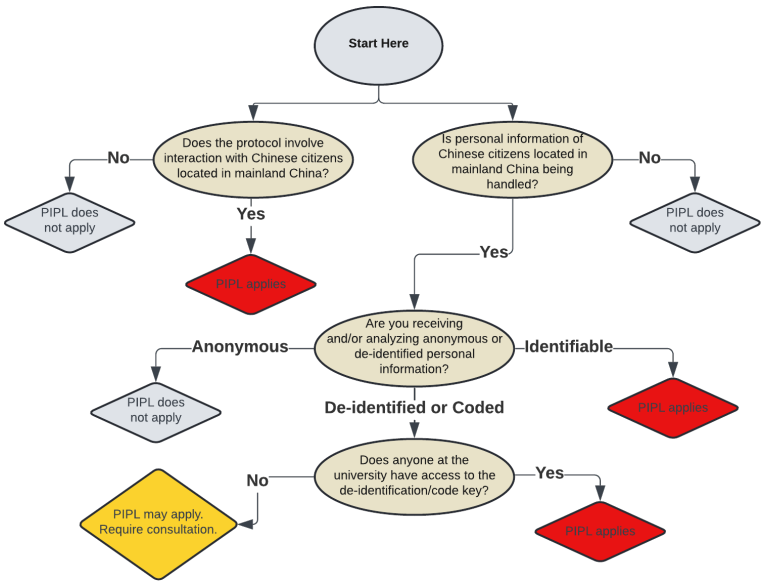
When must VU researchers comply with PIPL?

VU researchers must comply with PIPL when they handle personal information and/or assess the behavior of Chinese citizens located in China. This applies if the research involves collecting, storing, using, analyzing, or transferring personal data of Chinese citizens, regardless of where the researcher is based at the time of data collection or data processing.

PIPL defines personal information as the various kinds of information related to identified or identifiable natural person, whether recorded by electronic or other means, excluding the anonymized information processed anonymously. Processing of personal information includes the collection, storage, use, processing, transmission, provision, publication, and erasure of personal information.

When the VU HRPP receives a protocol subject to PIPL regulations, researchers will be required to consult with an expert familiar with PIPL's application in human subjects research. This consultation must be documented using the VU HRPP Local Context Consultation Form and submitted along with the protocol for IRB review. Additional approvals from other university units may also be necessary before the researcher can initiate the study.

PIPL Decision Tree



How does the Personal Information Protection Law (PIPL) address participant rights, informed consent, and data collection requirements?

Under PIPL, individuals have rights over their personal data, including access, correction, withdrawal of consent, and deletion of collected data. Specifically, PIPL requires that consent clearly outlines the purpose and scope of data use, any third-party sharing, and potential data transfer outside China. It must be specific, informed, and voluntary, and participants must understand how their data will be used, stored, and protected by foreign entities, including potential risks involved in cross-border transfers. Additionally, researchers conducting secondary data analysis must ensure that the initial consent form covers the new research questions. Otherwise, they will be required to re-consent participants to use their personal data.

In particular, consent must be obtained for processing sensitive personal information, which can only be processed for a specific purpose and sufficient necessity. Sensitive personal information includes personal information that can easily lead to the harm to the security or dignity of natural persons when disclosed or illegally used, including biometrics, religious belief, specific identities, medical health, financial accounts, and location tracking information, and the personal information of minors under the age of 14.

What are the requirements for data security and privacy?

PIPL requires robust data security measures to protect participant privacy. Researchers must implement the safeguards to prevent unauthorized access or data breaches, especially when handling sensitive data. The safeguards may include, but are not limited to, strict access controls (e.g., multi-factor authentication and role-based permissions), minimizing data collection to only the necessary data points required to address the research question, anonymizing or coding sensitive research data, conducting regular security audits of data storage, implementing clear data retention and deletion policies, and notifying individuals immediately about breachers to ensure compliance and reduce risks.

What is a data transfer?

A “data transfer” refers to the act of transferring personal information of individuals located within China to a recipient outside of China. Data transfers include both physical and electronic transfer. Some examples of data transfers (though not an exhaustive list) are included below:

- A researcher traveling from China to the US with a laptop containing covered research subject personal information of individuals located within China;

- A researcher transmitting files containing covered research subject personal information of individuals located within China (whether through email, file sharing, or other means) from China to the US;
- A researcher located in the US accessing a database of covered research subject personal information of individuals located within China collected by a colleague in China.

Because a data transfer refers to the act of transferring personal information of individuals located within China, the transfer of de-identified and anonymized information does not constitute a data transfer subject to the PIPL's data transfer requirements.

What are the requirements for data transfer and localization?

China's PIPL requires strict compliance for cross-border data transfers, particularly for entities classified as Critical Information Infrastructure Operators (CIIOs), such as entities in industries like telecommunications, energy, finance, or other areas crucial to national security, or those handling large volumes of personal data, which must store data locally unless they meet specific government-approved conditions. For transfers abroad, entities must obtain the data subject's separate consent and do one of the following:

(i) complete a security assessment conducted by the CAC ("Security Assessment");

(ii) obtain certification for the transfer by a CAC-accredited agency ("Third Party Certification"); or

(iii) enter into standard contractual clauses ("SCCs") with the offshore data recipient and file these terms with a personal information impact assessment ("PIIA") report.

The PIPL requires data controllers to conduct personal information impact assessments (PIIA) and to retain the results and processing records (for three years) in the following circumstances:

- processing of sensitive personal information;
- using personal information to conduct automated decision-making;
- appointing a data processor;
- providing personal information to any third party ;
- public disclosure of personal information;
- overseas transfer of personal information; and
- any other processing activities that may have "significant impact to an individual".

A PIIA should include an assessment on:

- whether the purpose of use and means of processing is legitimate, proper and necessary;
- impacts and risks to individual's interests; and
- applicability of protection measures and risk.

Certain cross-border data transfers are not subject to the above legal mechanisms under specific circumstances based on the type of entity transferring the data, the sensitivity/importance of the data transferred, and the volume of data subjects whose personal information is included in the transfer. Given the fact-specific nature of these exemptions and the high threshold for data transfer compliance, researchers will be required to consult with legal counsel or other experts on PIPL's application to human subjects research in order to receive IRB approval.

REFERENCES:

1. https://ogc.mit.edu/latest/china-and-pipl-new-protections-and-rights-personal-information
2. https://secureprivacy.ai/blog/china-pipl-personal-information-protection-law
3. https://research.uci.edu/human-research-protections/assessing-risks-and-benefits/privacy-and-confidentiality/china-personal-information-protection-law/
4. https://personalinformationprotectionlaw.com/chapter-ii-rules-for-handling-personal-information/