**TC IRB Guidance for Researchers: China’s Personal Information Protection Law (PIPL) Compliance**

**Purpose**

This document is intended to assist investigators at Teachers College (TC) in determining whether the Chinese Personal Information Protection Law (PIPL) applies to their research projects, provides an overview of the regulation in the context of research, and offers guidance for ensuring compliance with PIPL. It also outlines key researcher responsibilities, data subject rights, and contact points for questions.

**Key Terms and Definitions**

* PIPL: The Personal Information Protection Law (PIPL) is a Chinese law that came into effect on November 1, 2021, establishing protections for the privacy and security of "personal information" from or about individuals in Mainland China.
* Mainland China: Refers to the continental landmass under the direct control of the People’s Republic of China (PRC), including the islands of Hainan Province and five major autonomous regions (i.e., Tibet, Inner Mongolia, Xinjiang, Ningxia, and Guangxi), but excluding the Hong Kong Special Administrative Region (SAR), Macao SAR, and Taiwan.
* Personal Information (PI): Any information related to identified or identifiable individuals. *It does not include anonymized information.*
* Sensitive Personal Information (SPI): Personal Information that, if leaked or misused, may cause harm to personal dignity or safety. Examples include:
  + biometrics
  + religious beliefs
  + specific identities
  + medical health
  + financial accounts
  + whereabouts
  + personal information of minors under the age of 14
* Anonymized Information: Personal information processed so that it is impossible to identify certain natural persons and that such identification cannot be recovered
* Data Subject: The individual whose personal information is being collected and processed.
* Handler: Individuals that autonomously determine handling purposes of personal information.
* Processing: Any operation performed on personal information, including collecting, storing, using, transferring, or deleting data.

**What Activities Fall Under PIPL?**

PIPL protects data from or about individuals in Mainland China. The following activities fall under PIPL:

* Collecting personal data from individuals in Mainland China.
* Processing personal data by an organization established in Mainland China.
* Monitoring the behavior of individuals in Mainland China.

**Applicability to Research**

If your research involves personal data from individuals physically located in Mainland China, PIPL applies. This includes:

* On-site research in Mainland China.
* Remote or virtual research (e.g., interviews, surveys, or focus groups) involving individuals in Mainland China.
* Secondary research use of previously collected personal data about individuals in Mainland China.
* Web-based recruitment or surveys that target or enroll individuals in Mainland China.

**Legal Basis for Processing Personal Information**

While consent is the primary legal basis under PIPL, other lawful basis for processing personal data include:

* Performance of a contract involving the data subject.
* Compliance with legal obligations.
* Protection of public interests.
* Responding to public health emergencies or significant public interests.

For research purposes, explicit and informed consent remains the most relevant basis.

**Consent Requirements Under PIPL**

Researchers must obtain valid consent for the collection and use of personal data for research purposes. Consent must be:

* Freely given, specific, informed, and explicit.
* Supported by clear and transparent statements about the purpose of the study and the types of personal data collected.
* Informing participants of their rights under PIPL.
* Separate and explicit consent is required for sensitive personal information (SPI) (e.g., biometrics, health data, financial data).

If the purpose of processing changes after consent is obtained, new consent must be sought.

**Rights of Research Subjects Under PIPL**

Research subjects have several rights under PIPL, which researchers must communicate and provide mechanisms to honor, including the right to:

* **Access, Correction, or Deletion**: Individuals can access their personal information, request corrections, and ask for data deletion under certain conditions.
* **Restrict Processing**: Individuals can restrict the processing of their personal information​.
* **Object to Processing**: Individuals can object to the processing of their personal information for specific purposes, including for research​.
* **Withdraw Consent**: Individuals can withdraw their consent at any time. Previously collected data may still be used as outlined in the consent document.
* **Data Portability**: Individuals have the right to transfer their personal information to another organization​ if technically feasible.
* **Explanation for Automated Decision-Making**: Individuals can request explanations for automated decision-making processes​ and can object to decisions or request human intervention.

**Data Security and Retention**

Researchers must implement appropriate technical and organizational measures to protect personal data. This includes:

* **Data Security**: Ensure that data is protected from unauthorized access, use, disclosure, alteration, or destruction. Measures should match the sensitivity of the data being handled.
* **Data Retention**: Specify how long personal data will be retained and the criteria for this period. Specify how long personal data will be retained and the criteria for determining this period. Data must be deleted or anonymized after the retention period unless there is a lawful basis for extended retention.

**Cross-Border Data Transfers**

When transferring personal information outside Mainland China, researchers must:

* **Obtain separate and explicit consent** from individuals for cross-border data transfers.
* **Ensure the receiving party** provides a level of protection equivalent to that under PIPL.
* **Conduct a security review** or obtain administrative approval for transferring large volumes of sensitive personal data or transferring data to organizations located in countries without an adequate level of protection.

Failure to meet these requirements can result in penalties or suspension of the research project.

**Personal Information Protection Impact Assessment (PIPIA)**

Researchers must conduct a **Personal Information Protection Impact Assessment (PIPIA)** when:

* Processing **sensitive personal information**.
* Transferring large volumes of personal information across borders.
* Engaging in data processing activities that may pose high risks to the rights and interests of data subjects.

The assessment should evaluate the impact of data handling practices, outline measures to mitigate risks, and be included as part of **Section IV Confidentiality Procedures & Participant Privacy** in the IRB application.

**Automated Decision-Making**

If your research involves automated decision-making, researchers must:

* **Inform individuals** if automated decision-making is used in the study (e.g., through algorithms).
* **Allow individuals** to object to automated decision-making and request **human intervention** in such processes.

Examples include automated grading, personalized survey responses, or data analysis using machine learning.

**Data Breach Notification**

In the event of a data breach, researchers are required to:

* **Notify the IRB and the individuals** affected as soon as possible.
* **Report the breach to Chinese authorities** if the breach involves a large volume of sensitive data or has serious consequences for the data subjects.

Clear protocols should be in place for data breach response and reporting.

**Third-Party Data Processors**

If researchers work with third-party service providers or external collaborators who process personal information:

* A **Data Processing Agreement (DPA)** or **Data Transfer Agreement (DTA)** must be in place.
* Researchers must ensure that third parties comply with **PIPL’s data protection standards**.

The agreement should define each party’s responsibilities and the safeguards in place to protect personal data.

**Penalties and Investigator Liability**

As per [Article 66](https://personalinformationprotectionlaw.com/PIPL/article-66/), non-compliance with PIPL can lead to:

* **Fines** of up to 50 million yuan (approximately $7.7 million) or 5% of the previous year’s revenue.
* **Personal liability** for individuals responsible for handling personal data, including suspension or cancellation of business licenses.

Researchers should ensure full compliance to avoid these penalties.

**IRB Application Information: Requirements**

1. **Description of Data Collection and Processing:**
2. **Specify if personal data from individuals located in Mainland China will be collected.**
   1. Example: This research involves the collection and processing of personal data from participants located in Mainland China.
3. **Detail the types of personal data to be collected, including any sensitive personal data** (e.g., biometric data, financial information, health data).
   1. Example: The personal data collected will include academic performance, health information, and location data.
4. **Explain the purpose of data collection and how the data will be used in the research.**
   1. Example: The purpose of collecting personal data is to analyze the relationship between socioeconomic background and academic performance. The data will be processed and analyzed for this research objective only.
5. **Legal Basis for Data Processing:**
6. **Identify the legal basis for processing personal data under PIPL.** The primary legal basis for processing is **explicit consent**; however, other basis may apply, such as performing a contract or public interest obligations.
   1. Example: The legal basis for collecting and processing personal data in this study is the explicit consent obtained from participants.
7. **For research involving human participants, informed consent is considered the lawful basis for collecting and processing personal data under PIPL.**
   1. Example: Explicit and informed consent will be obtained from all participants before data collection.
8. **Data Protection Measures:**
9. **Describe the technical and organizational measures implemented to protect personal data**, such as encryption, pseudonymization, or access controls.
   1. *Example:* Personal data will be protected by encryption during transfer and access controls limiting data access to authorized personnel only.
10. **Explain procedures for pseudonymization or anonymization of data, if applicable.**
    1. *Example:* All personal data will be pseudonymized after initial collection and de-identified before analysis to ensure privacy and confidentiality.
11. **Data Subject Rights:**
12. **Outline how the rights of data subjects under PIPL will be addressed, including:**
    1. **Right to access**: Participants can access their personal data at any time.
    2. **Right to rectification**: Participants can request correction of inaccurate or incomplete data.
    3. **Right to erasure**: Participants have the right to request the deletion of their data under certain conditions.
    4. **Right to restrict processing**: Participants can restrict how their data is processed.
    5. **Right to data portability**: Participants have the right to transfer their data to another entity.
    6. **Right to withdraw consent**: Participants can withdraw consent at any time without affecting the lawfulness of data processing based on prior consent.
13. **Explain how these rights will be communicated to and exercised by the participants:**
    1. *Example:* Participants will be informed of their rights in the consent document and provided with clear instructions on how to exercise these rights.
14. **Data Transfer:**
15. **Indicate if personal data will be transferred outside Mainland China and the safeguards in place for such transfers** (e.g., Data Use Agreements, Data Transfer Agreements).
    1. *Example:* Personal data may be transferred to Teachers College in the United States for analysis. The transfer will be protected by a Data Transfer Agreement (DTA) to ensure compliance with PIPL, and participants’ data will be de-identified prior to transfer.
16. **Separate explicit consent must be obtained for cross-border data transfers:**
    1. *Example:* Participants will be informed and asked to provide separate consent for any cross-border data transfers.
17. **Data Retention:**
18. **Provide the duration for which personal data will be retained** and the criteria used to determine this period.
    1. *Example:* Personal data will be retained for three years after the conclusion of the research, in compliance with Teachers College’s data retention policy, but it will be fully anonymized to prevent re-identification. After this period, data will be deleted.
19. **Explain if data will be retained for a longer period** due to legal, contractual, or research-related reasons.
    1. *Example:* If necessary, personal data may be retained beyond three years, but it will be fully anonymized to prevent re-identification.
20. **Template Text for IRB Application (to be included under Section IV Confidentiality Procedures & Participant Privacy):**
21. This research involves the collection and processing of personal data from participants located in Mainland China. Teachers College (TC) is responsible for both collecting and processing this data. The legal basis for collecting and processing this data is explicit consent obtained by the TC PI from the participants. The personal data collected includes [specify types of data, e.g., academic performance, socio-economic background, survey responses].
22. Participants will be informed of their rights under PIPL in the consent document, including access, correction, deletion, restriction, data portability, and withdrawal of consent.
23. *If automated processing is involved:* Automated decision-making will be used to [e.g., analyze academic performance data to identify trends]. Participants have been informed of their right to **object to such processing** and request **human intervention**.
24. The personal data collected will be identifiable at the point of collection. De-identification measures will be applied once the data is processed and analyzed, ensuring that the data cannot be traced back to individual participants before any potential data transfer outside of Mainland China.
25. ***If data transfer is involved****:* Any transfer of de-identified data to Teachers College in the United States or other international destinations will be covered by appropriate Data Use Agreements (DUAs) or Data Transfer Agreements (DTAs) to ensure compliance with PIPL and to safeguard the confidentiality of the data.

**Consent Document Information: Requirements**

1. **Purpose of Data Collection:**
2. Clearly state the purpose for collecting and using personal data in the research study.
3. **Types of Data Collected:**
4. Specify the types of personal data being collected, including any sensitive data categories such as biometrics, health information, or location data.
5. If applicable, include a clear explanation in the consent form, informing participants of their right to refuse automated decision-making and request human intervention.
6. **Rights of Data Subjects:**
7. Inform participants of their rights under PIPL, including:
   1. Right to access their personal data.
   2. Right to correct inaccuracies in their data.
   3. Right to request deletion of their data under specific conditions.
   4. Right to restrict or object to the processing of their data.
   5. Right to data portability, allowing participants to transfer their data to another organization when feasible.
   6. Right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.
8. **Data Security Measures:**
9. Briefly explain the security measures in place to protect personal data (e.g., pseudonymization, encryption, access controls).
10. **Data Sharing and Transfer:**
11. Inform participants if their data will be shared with third parties or transferred outside of Mainland China, and describe the safeguards in place:
    1. These safeguards may include separate consent for cross-border transfers, encryption during transfer, pseudonymization of personal data, and strict access controls to ensure that only authorized personnel can access data.
    2. Ensure that data processing agreements (e.g., Data Use Agreements, Data Transfer Agreements) are established with third parties involved in the transfer and processing of personal data.
12. **Duration of Data Retention:**
13. Indicate how long personal data will be retained and the criteria used to determine this retention period. Data must be deleted or anonymized after this period unless otherwise required by law.
14. **Contact Information:**
15. Provide contact details for the individual responsible for data protection (e.g., Data Protection Officer or PI) and instructions on how participants can exercise their rights under PIPL.
16. **Template Text for Consent Forms:**
17. Please refer to the TC IRB [**PIPL Consent Notice Template**](about:blank) for the information to be included at the end of the main consent form and above the applicable signature block.

**Contacts**

For PIPL-related questions, contact the IRB office at [irb@tc.edu](mailto:irb@tc.edu) or TCIT at [privacy@tc.columbia.edu](mailto:privacy@tc.columbia.edu).

**Resources & References**

* [PIPL Consent Notice Template](about:blank)
* [Personal Information Protection Law of the People’s Republic of China](https://personalinformationprotectionlaw.com/)
* [Teachers College, Columbia University Privacy Notice](https://www.tc.columbia.edu/policylibrary/policies/privacy-notice-8438834/)