SOP-R-013: TC IRB Standard Operating Procedure (SOP) for Compliance with China's Personal Information Protection Law (PIPL)

1. Purpose

This SOP outlines the procedures for ensuring compliance with China's Personal Information Protection Law (PIPL) for research conducted under the auspices of Teachers College (TC) involving personal information from individuals located in Mainland China.

2. Scope

This SOP applies to all TC researchers, faculty, staff, and students who collect, store, use, or process personal information from or about individuals in Mainland China as part of their research activities.

3. Definitions

- **Personal Information (PI):** Any information related to identified or identifiable natural persons, excluding anonymized information. *It does not include anonymized information.*
- **Sensitive Personal Information (SPI):** Includes biometric data, religious beliefs, medical records, financial information, and data related to minors under 14.
- **Mainland China:** The continental landmass under the direct control of the People's Republic of China, including Hainan Province and five autonomous regions (i.e., Tibet, Inner Mongolia, Xinjiang, Ningxia, and Guangxi) *but excluding* the Hong Kong Special Administrative Region (SAR), Macao SAR, and Taiwan.
- **Data Subject:** The individual whose personal information is being collected and processed.
- **Personal Information Handler:** refers to organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods.
- **Automated Decision-Making:** refers to the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, hobbies, or financial, health, credit, or other status, and make decisions [based thereupon].
- **De-identification** refers to the process of personal information undergoing handling to ensure it is impossible to identify specific natural persons without the support of additional information.
- **Anonymization** refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore.

4. Responsibilities

- **Researchers:** Ensure compliance with this SOP and PIPL requirements.
- **IRB Reviewers:** Evaluate research protocols for compliance with PIPL.

Rev 0
Effective Date: 10/16/24

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB

- **Data Protection Officer (DPO):** Oversee data protection strategies and ensure compliance.
- **IRB Office:** Provide support and guidance on PIPL compliance.

5. Procedures

5.1 Informed Consent

5.1.1 Preparation:

- Ensure the informed consent form includes clear and explicit consent language.
- Detail the purpose of data collection, use, retention, and sharing.
- Specify if Sensitive Personal Information (SPI) will be collected and justify its necessity.
  - Ensure separate consent is obtained for data transfers, publication, and processing of sensitive personal information.
- Inform participants of their right to withdraw consent at any time and the procedure for doing so.
- Outline the rights of data subjects under PIPL and how they can exercise these rights.

5.1.2 Consent Notice:

- Include a PIPL consent notice at the end of the informed consent form above the signature block.
- Use the approved template for the PIPL consent notice TC IRB PIPL Consent Notice Template

5.2 Data Collection and Handling

5.2.1 Data Minimization:

- Collect only the minimum necessary personal information for the research purpose.

5.2.2 Method of Collection:

- Clearly describe the method of data collection (e.g., online form, survey, interview).

5.2.3 Purpose Limitation:

- Use collected data strictly for the specified research purpose.

5.2.4 Data Transfer:

- State if personal information will be transferred outside of Mainland China and ensure compliance with PIPL's security review process. Separate, explicit consent must be obtained from participants for such transfers, and safeguards such as Data Use Agreements (DUAs) or Data Transfer Agreements (DTAs) must be in place.
- Separate explicit consent must be obtained for any transfer of personal data outside of Mainland China. For transfers of large volumes of sensitive personal information (SPI), a security review must be conducted to ensure the protection of data during and after transfer. Researchers must also ensure that appropriate safeguards, such as Data Use Agreements (DUAs) or Data Transfer Agreements (DTAs), are in place for the international transfer of personal data.

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB

- Cross-border transfers of sensitive personal information may also require approval from Chinese authorities. Researchers must check whether their project requires administrative approval

5.3 Data Security and Retention

5.3.1 Security Measures:

- Implement appropriate technical and organizational measures to protect personal information from unauthorized access, disclosure, alteration, or destruction.

5.3.2 Retention Period:

- Personal data must be retained only for the minimum period necessary to fulfill the research objectives unless a lawful basis for extended retention exists. The criteria for determining the retention period should be specified in the protocol, and researchers must justify why extended retention is necessary. If personal data is retained beyond the original purpose, anonymization or de-identification measures must be applied to safeguard the data.

5.3.3 Third-Party Access:

- When third parties (e.g., external vendors and contractors) process personal information as part of the research, a Data Processing Agreement (DPA) or Data Transfer Agreement (DTA) must be in place. These agreements should specify the responsibilities of third-party processors and include safeguards to ensure compliance with PIPL. Researchers must ensure that third-party data processors adhere to the same data protection standards required under the study's protocols.

5.3.4 Data Breach Notification:

- In the event of a data breach, the researcher must notify the affected participants, the IRB, and the relevant Chinese authorities promptly. Notification should include details about the breach, potential consequences, and measures taken to mitigate harm.

5.4 Data Subject Rights

Researchers must ensure that participants are fully informed of their rights under PIPL, including the right to access, correct, delete, restrict processing, and transfer their data. Researchers should use clear and accessible language in the consent form and provide a contact point for participants to exercise their rights. The following rights should be clearly communicated:

5.4.1 Access Rights:

- Inform participants of their right to access their personal information.

5.4.2 Correction Rights:

- Provide procedures for correcting inaccurate or incomplete personal information.

5.4.3 Deletion Rights:

- Inform participants of their right to request deletion of their personal information and the process for doing so.

5.4.4 Portability Rights:

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB

- Inform participants of their right to request that their personal data be transferred to another organization if technically feasible. Researchers must inform participants how to request such transfers.

5.4.5 Restrict or Refuse Processing Rights:

- Inform participants of their right to object to the processing of their personal information and outline the procedure, especially in cases of automated decision-making.

5.4.6 Withdraw Consent Right:

- Inform participants of their ability to withdraw their consent at any time and explain how this will affect their participation in the study.

5.5 Legal and Ethical Considerations

5.5.1 Legal Basis:

- Document the legal basis for data processing, including explicit consent, contractual necessity, legal obligations, or other permissible bases under PIPL.
- Researchers must justify their choice of the legal basis for each processing activity.
- If automated decision-making is involved in the research (e.g., algorithms, machine learning models), researchers must clearly explain this to participants in the consent form. Participants must be informed of their right to object to automated decisions and to request human intervention. Researchers must also provide participants with an explanation of the logic behind the automated processing and the significance and consequences of such processing.

5.5.2 Compliance with PIPL:

- Ensure all aspects of data handling comply with PIPL.

5.5.3 Transparency:

- Maintain transparency about how personal information will be used, shared, and protected.

5.5.4 Review by IRB:

- Ensure the protocol has been reviewed and approved by the TC IRB for compliance with PIPL and ethical standards.

5.6 Additional Considerations

5.6.1 Data Protection Officer (DPO):

- Designate a DPO if required by the scope of the research and provide their contact information.

5.6.2 Impact Assessment:

- A Personal Information Protection Impact Assessment (PIPIA) is required for high-risk data processing activities, such as processing sensitive personal information, conducting automated decision-making with significant impacts on individuals, or transferring personal data across borders. The PIPIA should assess the following:
  - The necessity of processing personal and sensitive data.
  - The risks to the rights and interests of data subjects.

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB

        - The measures in place to mitigate these risks, including encryption, de-identification, and access control.
        - Compliance with PIPL requirements and any other applicable laws.
        - Procedures for notifying participants in case of data breaches.
    - The completed PIPIA must be submitted to the IRB as part of the study's application.

5.6.3 Ongoing Monitoring:

- Researchers must implement continuous monitoring procedures to ensure compliance with PIPL throughout the research project. This includes regular reviews of data protection measures, updates to participant consent if research methods change, and ensuring compliance with retention, security, and transfer protocols.

6. Review and Approval Process

6.1 Submission: Researchers submit their protocol and informed consent forms to the IRB for review.

6.2 Review: IRB reviewers use the TC IRB PIPL Compliance Reviewer Checklist to ensure all PIPL requirements are met.

6.3 Approval: The IRB approves the protocol if it meets all compliance and ethical standards.

7. Documentation and Record Keeping

7.1 Record Retention: Maintain documentation of compliance efforts, consent forms, and data protection measures for at least three years post-study or as required by applicable regulations.

7.2 Compliance Records: Keep records of all data subject requests and actions taken in response.

8. Training and Awareness

8.1 Provide training to researchers on PIPL requirements and data protection best practices.

8.2 Refer researchers to the TC IRB Researcher Guidance for China's Personal Information Protection Law (PIPL) Compliance for detailed guidance.

Contacts

- **IRB Office:** irb@tc.edu
- **TC IT:** privacy@tc.columbia.edu

Resources

- TC IRB Researcher Guidance for China's Personal Information Protection Law (PIPL) Compliance
- TC IRB PIPL Consent Notice Template
- TC IRB PIPL Compliance Reviewer Checklist
- Personal Information Protection Law of the People's Republic of China
- Teachers College, Columbia University Privacy Notice

Teachers College, Columbia University
Institutional Review Board
525 W. 120th St. Box 151, New York, NY 10027
212-678-4105 | IRB@tc.edu | RH 13 | tc.edu/IRB