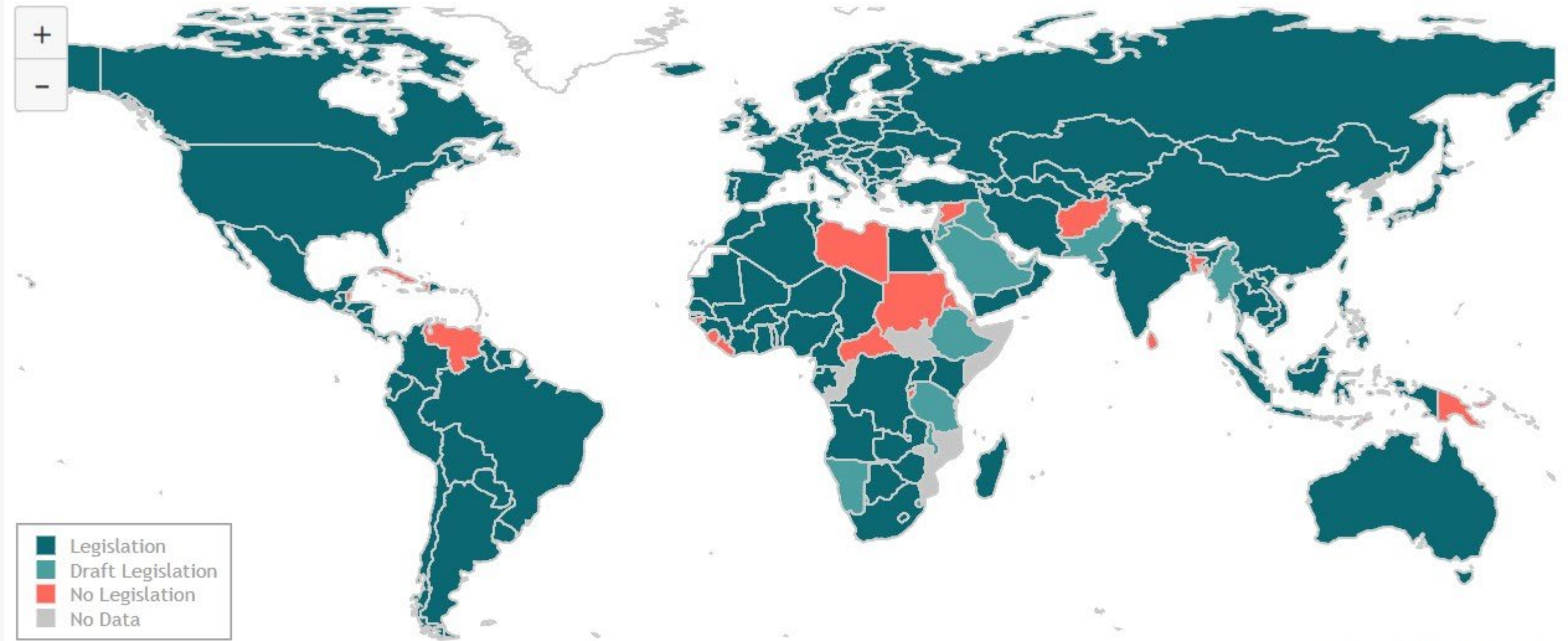

International Data Protection Laws— PIPL Compliance



*Tracy Dawson, JD, RN
Chief Privacy Officer
Office of Ethics and Compliance*

Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

China - PIPL



The Personal Information Protection Law (PIPL)

The Personal Information Protection Law was implemented in China effective November 1, 2021. It is similar to the EU GDPR in many respects. It imposes a broad set of data privacy requirements on the processing of personal information about individuals LOCATED within the borders of the People's Republic of China (PRC).

PIPL applies to entities outside of the PRC who are handling personal information of natural persons within the borders of the PRC:

- Where the purpose is to provide products or services to natural persons inside the borders
- Where analyzing or assessing activities of natural persons inside the borders
- Other circumstances provided in laws or administrative regulations

PIPL SUMMARY

PIPL

- Be informed about the processing of personal information (**notice**)
- **Obtain access** to and a copy of any personal information processed by handlers
- Able to **withdraw consent** to the processing of personal information where consent was previously provided
- Request correction of any personal information (**rectification**)
- **Request restriction** of certain uses of personal information
- Request handlers transfer personal information to others

Personal Information Includes (not limited to)

- Contact information (e.g., name, address, telephone number, e-mail address, internet protocol address and/or information that could be linked to an individual, etc.)
- Health information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Sexual orientation or beliefs
- Genetic data

Sensitive Personal Information Must Satisfy All Conditions

- Processing is necessary to achieve a specific purpose
- Strict protection measures are in place
- Data subjects are notified about the need to process their sensitive personal information and the impact such processing may have on their rights and interests
- Data subjects provide their specific separate consent to the processing of their sensitive personal information for the purpose disclosed

Sensitive Personal Information


Sensitive Personal Information is information that, if leaked or misused, could lead to discrimination, harm to physical/mental health, or damage to property or reputation.

Examples of SPI in China include:

- Biometric data (fingerprints, facial recognition)
 - Medical and health information
 - Financial account information
 - Personal information of minors under 14
 - Race, ethnicity, and religious beliefs
 - Precise location data
- Key Considerations:
 - Explicit consent is required for the collection, processing, or transfer of SPI.
 - Higher security measures must be applied when handling SPI. SPI has stricter requirements for cross-border transfers, including impact assessments and security reviews.



PIPL Compliance and Research

- If research activities conducted on behalf of Emory involve the collection, storage, processing, or transfer of Personal Information (PRC PI) or Sensitive Personal Information (PRC SPI) from individuals in the PRC, the PIPL will apply.
 - You must follow the appropriate policies and processes to ensure compliance with all applicable PIPL requirements.
 - Cross-border transfers of PRC PI or PRC SPI to Emory or other non-PRC locations require specific security, contractual, and control measures to be in place before the transfer of data.
- 

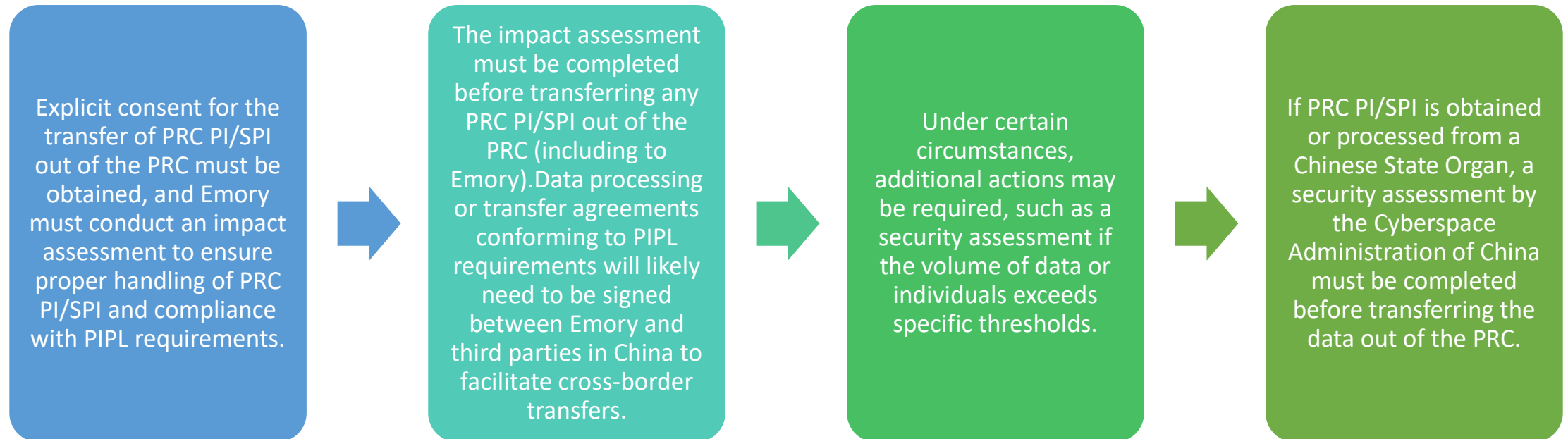
PIPL Consent Requirements

- Consent is expected to be the primary basis for acquiring PRC PI/SPI.
- Individuals must be fully informed about who will process their personal information, the purpose, scope, method of processing, their rights, and the retention period for their data.
- Explicit consent must be obtained, and if any changes occur in how personal information is processed, the individual must be notified, and re-consent obtained.
- Separate consent is required for transferring PRC PI/SPI out of the PRC (including to Emory).
- Individuals must be able to withdraw their consent easily, without it affecting their ability to receive other goods or services, unless consent is essential for providing those goods or services.

PIPL Compliance and Research

- It is important to identify the source of the PRC PI/SPI, which may be acquired directly from individuals (e.g., participation in research, interactions with the university website or social media), from a third-party collector (e.g., collaborators or partner institutions in the PRC), or from a Chinese State Organ.
- Different processing and security requirements may apply depending on the source of the PRC PI, with varying notice, consent, or processing rules based on the individual's identity (e.g., all personal information of minors under 14 is considered sensitive personal information, or PRC SPI).

Cross-Border Transfer of PRC PI/SPI



Penalties for Non- Compliance with PIPL

- **Fines:** Up to ¥50 million or 5% of annual revenue.
- **Business Suspension:** Temporary suspension of business operations.
- **Revocation of Licenses:** Business licenses may be revoked.
- **Civil and Criminal Liabilities:** Potential legal actions against the organization or individuals.
- **Public Exposure:** Violations may be publicly disclosed, leading to reputational damage

Contact Information

Tracy Dawson, JD, RN

Chief Privacy Officer

Tracy.s.Dawson@emory.edu

Phone: 404.727.4904

Office of Ethics and Compliance

Compliance@emory.edu

404.727.2398



QUESTIONS???