China’s Personal Information Protection Law - Compliance for Higher Ed

February 2022

Hunter Dorwart
Policy Counsel, FPF
Presentation Goals

1. Major differences between GDPR and PIPL

2. Minor nuances between the regimes

3. Administrative environment and context
Primary Regulatory Documents

- Personal Information Protection Law (PIPL) (个人信息保护法)
- PI Security Specification (信息安全技术个人信息安全规范)
- Personal Information Notification Consent Guidelines (信息安全技术个人信息告知同意指南)
- Draft Data Export Evaluation Measures (数据出境安全评估办法)
- Draft Online Data Management Regulations (网络数据安全管理条例)
## Comparison with GDPR

<table>
<thead>
<tr>
<th>Scope of Application</th>
<th>Processing Restrictions</th>
<th>Rights and Enforcement</th>
<th>GDPR Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extraterritoriality</td>
<td>Transfers</td>
<td>Individual Rights</td>
<td>More Flexible</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Legal Basis</td>
<td>Penalties</td>
<td>Similar</td>
</tr>
<tr>
<td>Controller/Processor</td>
<td>Accountability Measures</td>
<td>Claims</td>
<td>More Restrictive</td>
</tr>
</tbody>
</table>
# Areas of Major Divergence

<table>
<thead>
<tr>
<th>Legal Basis</th>
<th>Transfers</th>
</tr>
</thead>
<tbody>
<tr>
<td>- No legitimate interest</td>
<td>- Hard localization for certain controllers and certain types of data</td>
</tr>
<tr>
<td>- Conditions of valid consent</td>
<td>- Security assessment with regulator</td>
</tr>
<tr>
<td>- Separate consent</td>
<td>- Other transfer mechanisms</td>
</tr>
<tr>
<td>- Privacy policies</td>
<td></td>
</tr>
</tbody>
</table>
Applicability

• Data processing within territory of the PRC (Art. 2)
  ○ Personal information processing -
    ■ Similar broad definition to GDPR (i.e., identifiability)
    ■ Covers entire data life cycle
    ■ Applies to any data subject in China
  ○ Do not need an establishment for law to kick in (cf. GDPR Art. 3(1))

• Extraterritoriality (same as GDPR) (Art. 2)
  ○ Processing PI of individuals within China to:
    ■ Provide products or services to individuals in China
    ■ Analyze and assess the conduct of natural persons in China
  ○ Data Security Law (Art. 2)
    ■ Entities processing non-personal data outside of PRC that harm national security, the public order, or the rights and interests of individuals in China (i.e., important data)
Legal Basis

- **No legitimate interest**
  - Privacy policies
  - Notification requirements and opt-outs
  - No legitimate interest assessment

- **Consent-centric framework**
  - Primary lawful ground in practice
  - Most regulatory guidance to date
  - Broad overlap with GDPR
  - Subject to many exceptions in the PI Specification (e.g., national security)

- **Other lawful grounds (PIPL Art. 13)**
  - Necessary to conclude on a **contract** to which the individual is a party, or as necessary for carrying out **HR management** in accordance with labor rules systems and collective contracts;
    - Cf. EDPB 2019 guidance (maybe persuasive)
    - No current guidance on HR systems
  - Necessary to respond to **public health incidents** or to protect natural person security in their **lives, health, and property** in an emergency;
    - Cf. GDPR vital interests
    - No current guidance
Conditions of Valid Consent

- **Voluntary** - PI Specification Art. 3.6
  - Express - clear affirmative act, writing, or oral agreement (e.g., privacy policy)
  - Implied - no definition
  - Can’t be deceptive, misleading or coercive.

- **Informed** - PIPL Art. 18
  - More flexible than GDPR
  - Sensitive information must be clearly distinguished when collected/processed
  - State secrets and confidentiality exception (Art. 18)

- **Clear and specific**
  - Made public and easy to read and save.
  - Bundling (PI Specification Annex C)
    - Can bundle for “core” services but not “auxiliary” services
    - Functions essential to the product or service
Exceptions to Consent

- PI Specification Art. 5.6 - Big list, adds to PIPL.
  - Laws and regulations specify otherwise
  - National security or defense
  - Public security, public health, or major public interests (i.e., Covid-19)
  - Criminal investigations and prosecutions
  - Public information (i.e., data subject, news, or government)
  - Essential for operation of product or service
  - Academic research for public interests*

- Caveat -
  - PI Specification mentions *collection* and *use* but not *transfer* or *disclosure*.
  - Only two explicit exceptions to consent for transfers (Art. 35 Draft Online Data Security Management Regulations)
    - Concluding a contract where the data subject is a concerned party
    - Vital interests
Separate Consent

● Conditions triggering requirement (PIPL):
  ○ Sharing PI with another entity (Art. 23)
  ○ Public disclosures (Art. 25)
  ○ Sensitive information (Art. 29)
  ○ Cross-border transfers (Art. 39)
  ○ Facial recognition technologies (Art. 26)
  ○ Use of algorithms to push personalized content*

● Definition - Draft Online Data Security Management Regulations (Art. 73(8))
  ○ Obtaining consent for each item of PI relating to the specific processing act in question.
  ○ Cross-border exception (Art. 36)
    ■ Can obtain during initial notification if data subject is explicitly informed of the transfer
Sensitive Data

- Closely aligned with GDPR:
  - Harm and discrimination against a data subject’s personhood or property (Art. 28)
  - Processing only for specific purposes and when sufficiently necessary (Art. 28)
  - Need explicit consent for processing (subject to exceptions)

- Divergences and Nuances
  - Open list, PI Specification Annex B has unique identification guidance
  - Possibly need “written consent” in future administrative measures
  - Need to encrypt sensitive PI for transmission and storage under Chinese national encryption standards and store biometric data separately from identity data

- Exceptions:
  - General consent exceptions apply but with caution (e.g., national security, public health emergencies, protecting health or life of data subject)
  - No formal guidance on the interplay of these exceptions with sensitive data
Health and Research Data

- PI Specification Consent Exception:
  - When necessary for an academic research institute to conduct statistical or academic research in the public interest (Art. 5.6)
  - Scope of research must be reasonably related to collection purpose (Art. 7.3(a))
  - Data must be de-identified if research is made publicly available (Art. 7.3(a))
Transfers and Localization

Type of Controller

Critical Information Infrastructure Operator

Special Controllers

Large data controller (1m individuals)

“General” Data Controller

Type of Data

Localization

Large Transfers (100k Individuals; 10K Sensitive)

Important Data

Transfer Requirement

Security Assessment

Certification

SCCs

Other Measures
Definition of Transfer

- Not explicitly defined under the PIPL.
  - Numerous laws and regulations refer to “providing information abroad” (向境外提供).

- Three transfer scenarios outlined in 2017 Draft Cross-Border Transfer Guidelines
  - When data generated in China is stored outside China
  - When a copy of the data is provided to entities not subject to Chinese jurisdiction.
  - When the data is stored in China but can be accessed and viewed outside of the country.
Critical Information Infrastructure Operators (CIIOs)

● Definition (CII Regulations Art. 2) -
  ○ “Operators” of “important” network infrastructure and information systems in “important” industries.
  ○ Controllers, if damaged or suffers a data leakage will severely harm national security, the economy, or the public interest.

● Two Step Test -
  ○ Explicit Listing
    ■ Telecommunications, energy, transportation, water, finance, public services, e-government, national defense science, technology and industry.
  ○ Balancing
    ■ Importance of business
    ■ Extent of harm
Important Data

● Definition -
  ○ Data that can endanger national security or the public interest once tampered with, destroyed, leaked, or illegally obtained or used.
    ■ Article 73(3) Online Data Security Management Regulations.
    ■ Important Data Classification Guideline.
  ○ Broad, open-ended.
  ○ Not personal information or state secrets.

● Identification -
  ○ Illustrative list (Art. 73(3)).
  ○ Purpose of data
  ○ Security threats and risks
  ○ Could be implicated in research missions.
Additional Obligations

- Notification:
  - Recipient’s name and contact information
  - Method of exercising rights
  - Contemplated entrusted processing (i.e., purpose, methods, and scope of processing)
  - Controller bears responsibility

- Reciprocity
  - Controller must ensure recipient meets level of protection provided in PIPL.
    - Processing agreements
    - Inspections
  - No need to ensure recipient jurisdiction has equivalent level of protection
    - But CAC will consider this in its security assessment.
Security Assessment (CAC)

- Draft Data Export Evaluation Measures (Art. 5-13)
  - **Step one** - self transfer impact assessment
    - Legitimacy and necessity of transfer (purpose, methods, scope).
    - Quantity and type of transferred data and risks to national security or individuals' rights.
    - Technical measures to prevent risks.
    - Responsibilities of overseas recipients (i.e., transfer agreement)
    - Risk of data breach or abuse after transfer.
  - **Step two** - apply for the assessment with national CAC (declaration form, self-assessment report, transfer contract)
  - **Step three** - CAC undertakes assessment
    - **7 days** - national CAC gives indication of receipt
    - **45 days** after receipt - local CAC publishes results (with possible extensions)
    - Valid for **2 years**, unless there is a material change in the transfer arrangement or the legal environment of the recipient country.
    - Must re-apply within **60 working days** of the expiration of the assessment.
Data Breach Notification

- **Triggering Event (Art. 57 PIPL)**
  - When the leak, alteration or loss of PI occurs or is likely to occur.
  - Unlike GDPR, it does not matter if the breach is unlikely to result in a risk to rights and freedoms of the data subject.
  - Must always take immediate remedial action.

- **Notification Requirements (Art. 57 PIPL)**
  - Must **always immediately** notify local regulatory departments and take (CAC and possible MOE).
    - No 72 hour obligation. PIPL does not define “immediately”
  - Do not need to inform individuals of breach if remedial measures can effectively avoid the harm, even if **risk of harm** is high (cf. Art. 34 GDPR).
  - Must provide:
    - Types of information, reasons, and harms caused.
    - Remedial measures and method for DS to reduce harm.
    - Contact method.
Data Breach Notification (2)

- Additional Obligations (Draft Online Data Security Management Regulations)
  - Must notify individuals if harm occurs within **three working days** (Art. 11)
    - Note, PIPL provisions take priority: if harm is avoided, no need to notify.
  - Data breach involving important data or PI of 100,000 or more individuals (Art. 11):
    - Must notify CAC within **8 hours** (data quantities and categories, possible effects, response measures planned or adopted)
    - Must file a report with CAC within **5 working days** after incident response (incident’s cause, harmful consequences, responsibility assessment, improvement measures).
  - Response mechanisms, (e.g., incident reporting, contingency plans, organized training).
Minor Areas of Divergence

**DPIAs**
- Sensitive personal information processing
- ADM processing
- Controller/processor relationships
- Public disclosures
- Cross-border transfers

**DPOs**
- Main business involves PI processing and has 200+ employees
- Processes PI of 1 million+ individuals in one year.
- Processes sensitive PI of more than 100,000 people.

**Entrusted Processing**
- Controller bears liability for noncompliance
- Processor must employ necessary measures
- Joint controllers*
  - PI Specification Art. 9.6(b)
  - Processor who collects data on behalf of controller without obtaining consent is deemed joint controller.

* Joint controllers refer to PI Specification Art. 9.6(b)
Administrative Environment

● Regulators -
  ○ Cyberspace Administration of China (CAC)
  ○ Ministry of Industry and Information Technology (MIIT)
  ○ Ministry of Education (MOE)*

● Systemic Considerations -
  ○ Different legal environment and expectations
    ■ Strong emphasis on security and public order
    ■ Need to have good relationship with regulators (discretion and authority)
    ■ Possible sensitivity with student data
  ○ Recent regulatory reversal
    ■ Aligned with goals of 14th FYP
    ■ Prevent disorderly expansion of capital, promote healthy development of digital economy
    ■ Address “barbaric growth” of Internet platforms leveraging Big Data and privacy harms to citizens.
  ○ Size and funding of regulators
    ■ CAC has large budget and personnel.
Key Enforcement Trends

- Domestic IT companies, platforms, and mobile APPs:
  - Improper collection/use, inadequate consent, inadequate privacy policies
  - Unauthorized data transfers or inadequate security measures.
  - Chance to rectify, enforcement after deliberate failure or no excuse.

- Foreign firms:
  - No big examples yet.
  - Could target universities or vendors given importance.
  - Onsite inspections not uncommon
Thank You!

Questions: Hedorwart@fpf.org