McDermott Will & Emery

PIPL - A REVIEW OF CHINA'S NEW PRIVACY LAW AND INSIGHTS INTO ACHIEVING COMPLIANCE AND MANAGING RISKS

MIKE MORGAN

WENDY ZHANG

BILL DUMMETT

November 18, 2021

mwe.com

SPEAKERS

MIKE MORGAN

Partner
Los Angeles
+1 310 551 9366
mmorgan@mwe.com

WENDY ZHANG

Associate
Los Angeles
+1 310 788 6012
wwzhang@mwe.com

BILL DUMMETT

Associate General Counsel &
Chief Privacy Officer
Genesys
bill.dummett@genesys.com

AGENDA

- Overview of data privacy and protection landscape
- PIPL obligations
- Considerations for compliance and managing risk

OVERVIEW OF DATA PRIVACY AND PROTECTION LANDSCAPE

PERSONAL INFORMATION PROTECTION LAW (PIPL)

- Effective: November 1, 2021
- Similar in subject and scope to the EU's GDPR
- Extraterritorial applicability
- Governs the processing of personal information, including sensitive personal information
- Stronger reliance on consent for processing, including for collecting, using, and transferring personal information
- Potential complications for transferring personal information out of China

See generally, Personal Information Protection Law (effective Nov. 1, 2021), Ch. I-III (China) (hereinafter, PIPL).

CYBERSECURITY LAW (CSL) AND DATA SECURITY LAW (DSL)

CSL: Effective June 1, 2017

- Provides framework for network security obligations
- CSL covers “network operators” in China as well as suppliers of network products and services
  - Network operators is defined broadly, covering essentially anyone owning or operating a computer system network
- Includes very high-level requirements for protecting personal information

DSL: Effective September 1, 2021

- Regulates the use and security of all data and data activities
- Based on data categorization and classification systems
- Allows for industry-specific rules and regulations, especially for industries like telecommunications, transportation, natural resources, hygiene and health, education, and technology

- Both primarily apply to activities within China with minimal extraterritorial reach

See generally, Cybersecurity Law (China), Data Security Law (China).

PIPL OBLIGATIONS

LOST IN TRANSLATION

Personal Information Processor

- Similar to “data controller”
- Refers to any organization or individual that independently decides the processing purpose and processing method in personal information processing activities

Disclose

- Narrower than common English understanding of the term
- Means something like “publicizing”
- Does not include, for example, sharing personal information with a service provider for purposes of performing agreed upon services
- Certain obligations under PIPL triggered if “disclosing”

Individual Consent / Specific Consent

- Means a distinct, separate consent that cannot be lumped into a generic consent form

See PIPL Art. 73, 13, 14.

APPLICABILITY

- Applies to processing of "personal information" which is broadly defined as "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person"
  - Does not include anonymized data
- Applies to processing of personal information within China
- Applies to extraterritorial processing of personal information of Chinese residents if processing is for:
  - The purposes of providing products and services to Chinese residents
  - Analyzing and evaluating the behavior of Chinese residents
  - Other circumstances under laws and regulations (not yet specified)

PIPL Art. 3, 4.

PROCESSING REQUIREMENTS

- Adhere to personal information processing principles
  - Lawfulness
  - Collection and Purpose Limitation
  - Transparency
  - Accountability
  - Security

- Requires legal basis for processing personal information
  - Consent
  - Processing is necessary for performance of a contract, including for employment-related purposes
  - To perform statutory duties
  - To respond to public health emergencies, protect life, health, and property
  - Carry out news reports or other acts for the public interest
  - Processing as disclosed by individual within reason
  - Other circumstances permitted under law

PIPL Art. 5-7, 13.

NOTICE AND CONSENT

- Provide notice prior to processing
- Notice must include:
  - Name and contact information of PIP
  - Purpose of processing personal information
  - Processing method
  - Types of personal information processed
  - Retention periods
  - Methods and procedures for exercising privacy rights
  - (Other information not yet identified under laws and regulations)

- If relying on consent as legal basis for processing:
  - Consent must be knowing and voluntary
  - Written consent only required where laws and regulations require it
- Must obtain consent again if the processing purpose, methods, or types of personal information processed change
- Individual has right to withdraw consent
- Individual consent required under certain circumstances
  - Processing sensitive data
  - Disclosing personal information

PIPL Art. 13-17.

SPECIAL CONSIDERATIONS FOR SENSITIVE DATA

- Sensitive data defined as “personal information that, once leaked or used illegally, can easily lead to the infringement of personal dignity of natural persons or the harm of personal property, safety”
  - Includes: biometrics, religious beliefs, specific identities (*e.g.*, ethnic identity), medical health, financial accounts, information about whereabouts or location, and personal information of minors under the age of 14
- Can only process sensitive data if there it is necessary for a specific purpose
- Requires individual consent
- Must also notify individuals of the necessary purpose and impact on personal rights and interests

PIPL Art. 28-31.

PRIVACY RIGHTS (PIPL VS. GDPR VS. CCPA)

	PIPL	GDPR	CCPA
Right to non-discrimination		*Implicit Right*	X
Right to Know	X	X	X
Right to Access/Copy	X	X	
Right to Data Portability	X (with fewer requirements)	X	X
Right to Correction	X	X	
Right to Object/Restrict Processing	X	X	
Right to limit Automated Decision Making	X	X	
Right to Opt-Out of Sale			X
Right to Erasure	X	X	X
Passes to Next-of-Kin upon Death	X		

PIPL Art. 14, 16, 24, 44, 45, 46, 47, 49.

GDPR Art. 13-17, 20-21 (European Union, 2016).

CCPA 1798.100-1798.125 (California, 2018).

PERSONAL INFORMATION IMPACT ASSESSMENT

- a.k.a. “DPIAs”
- Necessary before processing in following scenarios:
  - Processing sensitive personal information
  - Conducting automated decision-making
  - Providing personal information to other PIPs or “trustees” (akin to “data processors”)
  - Disclosing personal information
  - Providing personal information abroad
  - Other personal information processing activities with a major impact on individuals
- Must consider:
  - Whether processing purpose and method are legal, proper, and necessary
  - Impact on personal rights and security risks
  - Whether protective measures are legal, effective, and compatible with degree of risk
- Retain records of the assessment for three years

PIPL Art. 55, 56.

UTILIZING THIRD-PARTY TRUSTEES

- PIPs must conduct PIIAs prior to sharing and is responsible for "trustee's" processing activities
- Contractual provisions:
  - Describe the purpose, time limit, processing method, types of personal information processed, protection measures, and rights and obligations of the parties, including assisting PIP in fulfilling its obligations under PIPL
  - "Trustees" may not process personal information beyond the agreed upon purposes and must return or delete the personal information upon termination of the agreement
  - "Trustees" are prohibited from delegating to others without consent of the PIP

PIPL Art. 21, 55.

CROSS-BORDER TRANSFER REQUIREMENTS

- Must receive permission from Chinese competent authorities before transferring data stored in China to foreign law enforcement or judicial agencies
- Must provide notice to individuals and obtain specific consent for transfer
- Conduct Personal Information Impact Assessment

- Meet at least one of the following conditions;
  - Treaty between PRC and receiving state's government
  - Undergo security assessment conducted by government (mandatory requirement for CIIOs and organizations that process large volumes of information, but threshold not yet specified)
  - Obtain personal information protection certificate – qualified professionals not yet designated
  - Contract with a foreign organization (Standard Contractual Clauses) – not yet published
- Other conditions provided in laws or administrative regulations or by CAC

PIPL Art. 38, 39, 55.

CYBERSECURITY REQUIREMENTS

- Create internal management system and operating procedures
- Implement data classification management
- Adopt security technical measures like encryption and de-identification
- Regularly conduct education and training
- Create and implement incident response plans
- Regularly conduct compliance audits
- Conduct personal information impact assessments
- Designate DPO (threshold not yet specified) and/or local representative
- Consider requirements set forth in CSL and DSL

PIPL Art. 51-54.

INCIDENT RESPONSE

- Security incident includes “leakage, tampering, or loss” that occurs or that *may occur*
- PIP must develop and implement incident response plan
- PIP must take remedial actions and notify regulator:
  - Type, reason, and risk of harm
  - Remedial measures to reduce harm
  - Contact information
- If measures taken effectively avoid harm, notice to individuals is not required, but the regulator has the right to require PIP to notify if the regulator believes harm may occur

PIPL Art. 57.

ENFORCEMENT AND PENALTIES

- Government enforcement
  - Up to 50 million RMB (~7.8 million USD) or 5% of annual revenue
  - Up to 1 million RMB (~157K USD) for the person directly responsible
  - PIP may have opportunity to remedy alleged violation without penalty, after initial notification of violation by regulator
- Civil liability for damages and other torts
  - Burden of proof is on the PIP to show that it is not at fault
  - Private right of action where PIP refuses to honor privacy right
- Potential criminal liability
- Concerns of possible selective enforcement
  - Historically, potentially higher enforcement risk for big tech, big data, and Chinese companies seeking to be listed on foreign exchanges

PIPL Art. 66, 70, 71.

CONSIDERATIONS FOR COMPLIANCE AND MANAGING RISK

CONSIDERATIONS FOR COMPLIANCE

- Map data flow and conduct data classification
- Designate representatives and officers
  - DPO and/or local representative or entity
- Update privacy policy
- Assess and update consent mechanisms
  - Incorporate consent into existing processes
  - Identify where additional individual consent might be required
- Develop, implement, and/or update consumer request procedures

CONSIDERATIONS FOR COMPLIANCE CONT.

- Update data processing agreements with vendors/service providers/processors
- Identify circumstances when personal information impact assessments are necessary and implement procedures for conducting them
- Conduct regular (consider: annual) compliance audits
- Update incident response procedures
- Consider risk-based approach for transferring data out of China in absence of published SCCs or designated professionals for issuing certificates
  - Consider avoiding export of personal data from China, including via changes to systems infrastructure and data flows as well as use of outsourced China-based providers

THANK YOU / QUESTIONS?

mwe.com

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery* (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.
*For a complete list of McDermott entities visit mwe.com/legalnotices.

©2021 McDermott Will & Emery. All rights reserved. Any use of these materials including reproduction, modification, distribution or republication, without the prior written consent of McDermott is strictly prohibited. This may be considered attorney advertising. Prior results do not guarantee a similar outcome.