香港城市大學
City University of Hong Kong
Innovating into the Future

Prof Zhu Guobin, PhD

School of Law City University of Hong Kong

Data Privacy Law in the Mainland

OUTLINE

I. Introduction — No Single Comprehensive Data Protection Law

II. “3+N” Framework in Mainland Privacy Law

III. Personal Information Protection Law

IV. Transferring Personal Information out of the Mainland

V. Emerging Technologies and Data Privacy Updates

I. Introduction

No Single Comprehensive Data Protection Law

A. Three Pillars of the System of Law

- Cybersecurity Law (網絡安全法, CSL, adopted in 2016 and effective in 2017)
  - Focusing on Network Operations Security (Operations Security for Critical Information Infrastructure)
  - Network Information Security
- Data Security Law (數據安全法, DSL, 2021)
  - Classification of Data by Importance
  - Emphasizing Security and Openness of Government Data
- Personal Information Protection Law (個人信息保護法，PIPL, 2021)
  - Providing Principles and Rules Governing Data Processing
  - Highlight of Individual’s (Data Subject’s) Rights
  - Clarification of Public Authorities’ Information Protection Obligations

B. Development of the Pillar Laws

- State Council Information Office deployed legislative research on the Personal Information Protection Law in 2003.

- “Decision of the Standing Committee of the National People‘s Congress (NPCSC) on Strengthening Network Information Protection” in 2012

- Continued decentralised legislation regarding personal information protection: the 9th Amendment to the Criminal Law (2015); the Cybersecurity Law(2017), the E-Commerce Law (2018), the Civil Code (2020), the newly revised Consumer Protection Law (2024), etc

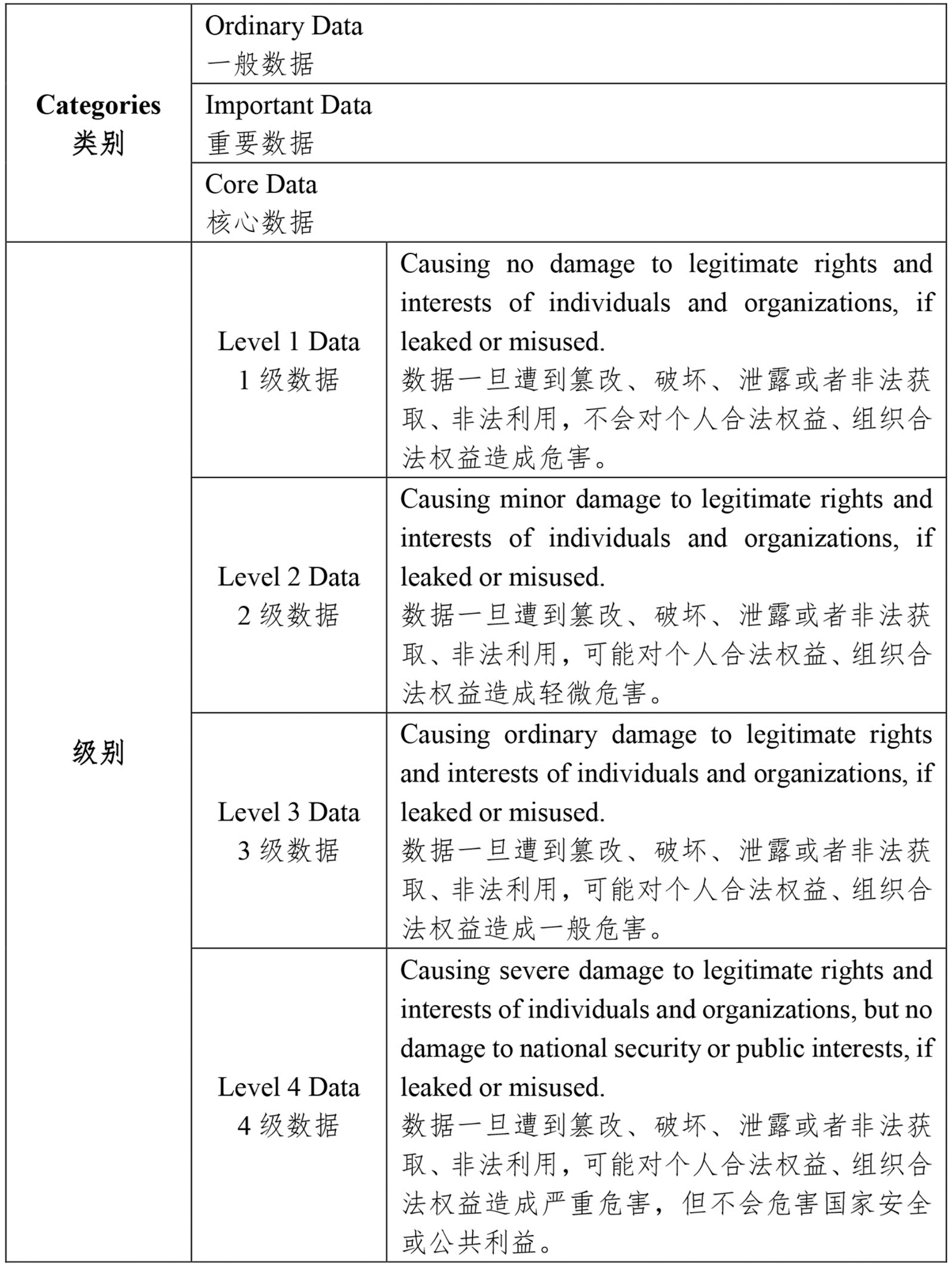
- Inclusion of the Personal Information Protection Law in the “Legislative Plan of the NPCSC" in September 2018, leading to its adoption in 2021.

C. Connections of the Three Main Pillars

- 1. Cybersecurity Law (CSL, 2017): The primary purpose is to regulate activities of network operators

  - Key Outcome: Multi-Level Protection Scheme [MLPS]

Network level	The consequence once the network is destroyed
Level 1	- Damage to the legitimate rights and interests of relevant citizens, legal persons and other organizations
Level 2	- Serious damage to the legitimate rights and interests of relevant citizens, legal persons and other organizations; or - Harm to social order and public interests;
Level 3	- Particularly serious damage to the legitimate rights and interests of relevant citizens, legal persons and other organizations; - Serious harm to social order and public interests; or - Against the hazards of national security;
Level 4	- Particularly serious harm to social order and public interests; or - Serious hazards to national security;
Level 5	- Particularly serious harm to national security.



Categories **类别**	Ordinary Data 一般数据	
	Important Data 重要数据	
	Core Data 核心数据	
级别	Level 1 Data 1 级数据	Causing no damage to legitimate rights and interests of individuals and organizations, if leaked or misused. 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，不会对个人合法权益、组织合法权益造成危害。
	Level 2 Data 2 级数据	Causing minor damage to legitimate rights and interests of individuals and organizations, if leaked or misused. 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成轻微危害。
	Level 3 Data 3 级数据	Causing ordinary damage to legitimate rights and interests of individuals and organizations, if leaked or misused. 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成一般危害。
	Level 4 Data 4 级数据	Causing severe damage to legitimate rights and interests of individuals and organizations, but no damage to national security or public interests, if leaked or misused. 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，但不会危害国家安全或公共利益。

- 2. Data Security Law (DSL, 2021): Expanding regulation to all data processing activities
  - Key Outcome: Data Classification and Grading System: Ordinary Data, Important Data, Core Data
    - National Standard: "Practice Guidelines for Cybersecurity Standards — Guidelines for Network Data Classification and Grading" (2021.12);
    - Specifically in the "Guidelines": 6.2 Basic classification rules (Categories), and 6.3 General data classification rules (Levels), as shown in the chart.

- 3. Personal Information Protection Law (PIPL, 2021): Regulating personal information protection in the process of processing activities
  - Applicability
    - Identified and Identifiable personal information of natural persons;
    - Art. 4: Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymisation handling.
  - Range (and extraterritoriality)
    - Activities conducted in China or;
    - Outside of China if,
      - a. the purpose of the processing is to provide products or services to natural persons in China;
      - b. the purpose of the processing is to analyze and evaluate the behaviour of natural persons in China; or
      - c. other circumstances provided by laws and administrative regulations. (Art. 3)

D. Conclusion

- Cybersecurity Law: regulates the environment; functions as a standard in classifying importance level of network systems

- Data security law: provides a guidance for secured data flow; functions as standard categorization of data.

- PIPL has more functions of creating a “parallel legislation” that resembles GDPR, following the legislative measures of previous two laws in categorisation (sensitive/ non-sensitive information); it also provides more principles, rights and obligations, etc.

    - PIPL is more right-based.

II.
“3+N” Framework of the Mainland Privacy Law System

3 Main Laws	Other Regulations and Rules, & Normative Documents
• Cybersecurity Law (2017) • Data Security Law(2021) • Personal Information Protection Law (2021)	• Administrative Regulations • Departmental Rules • Regulatory Documents • Judicial Interpretations • National Standards

- Features
  - Well-established system
  - Wide coverage and sspecific contents
  - Need further detailed guidance to meet the challenges in the enforcement process
  - Strengthen the intensity of supervision

III.
Personal Information Protection Law with Comparative Analysis

A. Legal Principles

- **1. Legality,** Art 5, PIPL: The principles of legality, propriety, necessity, and sincerity shall be observed for personal information handling. It is prohibited to handle personal information in misleading, swindling, coercive, or other such ways.
- **2. Purpose limitation**. Art 6 para 1, PIPL : Personal information handling shall have a clear and reasonable purpose, and shall be directly related to the handling purpose, using a method with the smallest influence on individual rights and interests.
- **3. Minimum necessity**, Art 6 para 2, PIPL: The collection of personal information shall be limited to the smallest scope for realizing the handling purpose, and excessive personal information collection is prohibited.

- **4. Openness and transparency,** Art 7, PIPL: The principles of openness and transparency shall be observed in the handling of personal information, disclosing the rules for handling personal information and clearly indicating the purpose, method, and scope of handling.
- **5. Integrity,** Art 8, PIPL: The handling of personal information shall ensure the quality of personal information, and avoid adverse effects on individual rights and interests from inaccurate or incomplete personal information.
- **6. Accountability:** Art 9, PIPL: Personal information processors shall bear responsibility for their personal information handling activities, and adopt the necessary measures to safeguard the security of the personal information they handle.

- **Comparing with GDPR (The General Data Protection Regulation) (I)**

GDPR, Art 5	PIPL, Arts 5-9
• Lawfulness, Fairness, and Transparency • Purpose Limitation • Data Minimization • Accuracy • Storage Limitation • Integrity and Confidentiality • Accountability	• Legality • Purpose Limitation • Minimum Necessity • Openness and Transparency • Integrity • Accountability

- **Comparing with GDPR, cont.**
- GDPR adopted consent as a principle and set a whole chapter regarding principles other than basic values
  - Principles relating to processing of personal data
  - Lawfulness of processing
  - Conditions for consent
  - Conditions applicable to child’s consent in relation to information society services
  - Processing of special categories of personal data
  - Processing of personal data relating to criminal convictions and offences
  - Processing which does not require identification

B. Rules

- Core Rule: Notice-Consent (Art. 13), see next page
- Content of Notice: (Art. 17)
- The name or personal name and contact method of the personal information processor
- The purpose of personal information handling and the handling methods, the categories of processed personal information, and the retention period
- Methods and procedures for individuals to exercise the rights provided in this Law
- Other items that laws or administrative regulations provide shall be notified
- Exemptions (Art. 18): under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary; under emergencies.

- **Art 13 (PIPL): Personal information processors may only handle personal information where they conform to one of the following circumstances:**
  - (1) **Obtaining individuals' consent;**
  - (2) Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;
  - (3) Where necessary to fulfill statutory duties and responsibilities or statutory obligations;
  - (4) Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
  - (5) Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;
  - (6) When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law.
  - (7) Other circumstances provided in laws and administrative regulations.
  - In accordance with other relevant provisions of this Law, when handling personal information, individual consent shall be obtained. **However, obtaining individual consent is not required under conditions in items 2 through 7 above.**

- **Comparing with GDPR (II)**

GDPR	PIPL
Requirement of Consent in GDPR • Free to give • Specific • Informed • Show with a clear statement or positive behaviour	**Flaws in mainland practice under PIPL** • Less specification leads to fail to guarantee free to give e.g. WeChat system • Does not Comply with GDPR’s high standard of “Informed” e.g. Baidu Privacy Statement • The debatable case: First Case of Cookie Privacy (*Zhu Ye v. Beijing Baidu Netxun Technology Company*)

C. Sensitive Personal Information Protection Heightened

- Chapter II, Section II, PIPL: Rules for Handling Sensitive Personal Information敏感個人資訊的處理規則

- General Rules

  - Article 28: Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

  - Only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures, may personal information processors handle sensitive personal information.

- Consent and Exemptions
  - Article 29: To handle sensitive personal information, the individual's separate consent shall be obtained. Where laws or administrative regulations provide that written consent shall be obtained for handling sensitive personal information, those provisions are to be followed.
  - Article 30: Personal information processors handling sensitive personal information, in addition to the items set out in Article 17, Paragraph 1, of this Law, shall also notify individuals of the necessity and influence on the individual's rights and interests of handling the sensitive personal information, except where this Law provides that it is permitted not to notify the individuals.
- Rules for Minors
  - Article 31: Where personal information processors handle the personal information of minors under the age of 14, they shall obtain the consent of the parent or other guardian of the minor.

D. Specific Regulations on State Organs Highlighted

- Chapter II, Section III, PIPL: Specific Provisions on State Organs Handling Personal Information 國家機關處理個人資訊的特別規定
  - Art 33: This Law applies to State organs’ activities of handling personal information; where this Section contains specific provisions, the provisions of this Section apply.
- Scope and Limitations
  - Art 34: State organs handling personal information to fulfill their statutory duties and responsibilities shall conduct them according to the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfill their statutory duties and responsibilities.
- Notification Requirement and exemptions
  - Art 35: State organs handling personal information for the purpose of fulfilling statutory duties and responsibilities shall fulfill notification duties, except where circumstances as provided in Article 18, Paragraph I, of this Law exist, or where notification will impede State organs’ fulfillment of their statutory duties and responsibilities.

E. Rights of Information Subject / Individuals' Rights in Personal Information Processing Activities

- 1. The right of know and right to decide. Art 44
- 2. The right of access and replication. Art 45
- 3. The right of portability. Art 45 para 2
- 4. The right of correction and supplementation. Art 46
- 5. The right of deletion. Art 47
- 6. The right for an explanation. Art 48
- 7. The Right for the deceased. Art 49

- **Comparing with GDPR (III)**

GDPR	PIPL
Rights of Data Subject in GDPR • Section 1 Transparency and modalities • Section 2 Information and access to personal data • Section 3 Rectification and erasure • Section 4 Right to object and automated individual decision-making • Section 5 Restrictions	**One less considered point in PIPL** • Right to object; e.g. Cookie Case and Big Data Shashu (“殺熟”) • One seldom practiced point in PIPL • Right to be forgotten; e.g. only a limited number of governmental announcements deleting pandemic related personal information

F. Further Concerns

- 1. Didi case in 2021:
  - Illegal collection of screenshots from users' mobile albums, excessively collecting passengers’ facial recognition information, age, family relationships information and address information, analyzing passenger travel intentions without clear notification, frequently requesting irrelevant "phone permissions" when passengers use ride-sharing services and so on.

  - Result: In Jul 2021, Cybersecurity Review Office conduct cybersecurity review toward Didi company according to *Measures for Cybersecurity Review* 網路安全審查辦法 (adopted Dec 2021, effective Feb 2022). Upon further investigation, it was found that Didi violated the *Cybersecurity Law, Data Security Law,* and *Personal Information Protection Law*.

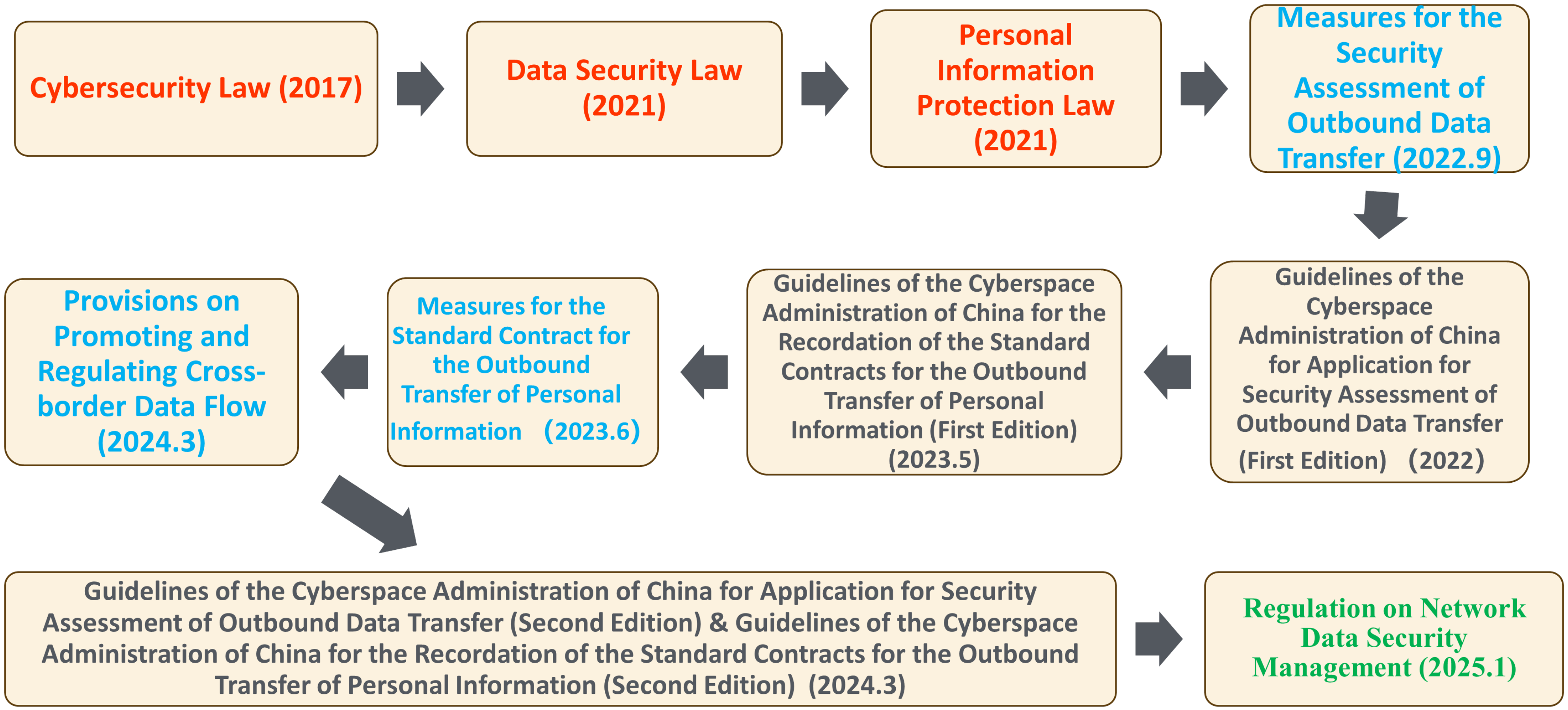
- 2. "AI face-changing" software case in 2024
  - Without the authorization of the plaintiff, the defendant used technical means to make a face-changing template based on the video released by the plaintiff without authorization, and then uploaded it to the "face-changing" APP involved in the case for users to pay for use, so as to make illegal benefits.
  - Analysis: The act of making a face-changing template is not a legal infringement of portrait rights. However, unauthorized use of other people's identifiable appearance videos constitutes the violation of the rights and interests of personal information.
    - Issues concerned:
    - (1) Lack of consent
    - (2) Right to know and the right to decide
    - (3) Unauthorized processing

IV.
Transferring Personal Information out of the Mainland

Overview

- Central Level—“3+N” & Legislative Development History (2017 -)
  Local Level—Take Great Bay Area for example
- Three basic systems — Security Assessment, Certification and Standard Contract
- Relevant Cases

A. Overview —
Legislative Development History - Central Level



Cybersecurity Law (2017)

Data Security Law (2021)

Personal Information Protection Law (2021)

Measures for the Security Assessment of Outbound Data Transfer (2022.9)

Guidelines of the Cyberspace Administration of China for Application for Security Assessment of Outbound Data Transfer (First Edition) (2022)

Guidelines of the Cyberspace Administration of China for the Recordation of the Standard Contracts for the Outbound Transfer of Personal Information (First Edition) (2023.5)

Measures for the Standard Contract for the Outbound Transfer of Personal Information (2023.6)

Provisions on Promoting and Regulating Cross-border Data Flow (2024.3)

Guidelines of the Cyberspace Administration of China for Application for Security Assessment of Outbound Data Transfer (Second Edition) & Guidelines of the Cyberspace Administration of China for the Recordation of the Standard Contracts for the Outbound Transfer of Personal Information (Second Edition) (2024.3)

Regulation on Network Data Security Management (2025.1)

A. Overview — Local Level

- Opinions of the State Council on Further Optimizing the Foreign Investment Environment and Increasing Efforts to Attract Foreign Investment 國務院關於進一步優化外商投資環境加大吸引外商投資力度的意見 (2023.7)
- Implementing Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) 粵港澳大灣區（內地、香港）個人資訊跨境流動標準合同實施指引(2023.12)
  - Issued by State Internet Information Office of China and Hong Kong Innovation, Technology and Industry Commission (ITIC) 國家互聯網資訊辦公室和香港創新科技及工業局, The first official document at the local level to make facilitative arrangements for the national data cross-border.
  - Exempting the requirement for security assessments of personal information transfers between Guangdong and Hong Kong, simplifying the content of Privacy Impact Assessment, and reducing obligations for overseas recipients.
  - Promotes the free flow of data between Guangdong and Hong Kong.
- Implementing Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Macao) (2024.9)
- Other regions, such as Beijing and Shanghai
  - Measures for the Classified and Graded Management of Cross-border Data Flow in the Lin-gang Special Area of China (Shanghai) Pilot Free Trade Zone (for Trial Implementation) (2024.2)
  - Several Measures of Beijing Municipality for the Administration of Cross-Border Data Flow Facilitation Services, announced by three Departments Including the Cyberspace Affairs Office of Beijing Municipality (2024.8)

B. Three Basic Systems —
Security Assessment, Certification and Standard Contract

- 1. Security Assessment
  - Cybersecurity Law, Art 37
  - PIPL Art 40
  - *Measures for the Security Assessment of Outbound Data Transfer*
- 2. Certification
  - PIPL Art 38(2)
  - *Measures for the Personal Information Protection Certification for the Outbound Transfer of Personal Information (Exposure Draft)*
- 3. Standard Contract
  - PIPL Art 38 (3)
  - *Measures for the Standard Contract for the Outbound Transfer of Personal Information*
  - *Many Guidelines…*

Comparison among Three Basic Systems under Provisions on Promoting and Regulating Cross-border Data Flow 《促進和規範資料跨境流動規定》

	Non-Critical information infrastructure operators				Critical information infrastructure operators
	Personal information <100,000	100,000< personal information < 1,000,000 / Sensitive personal information < 10,000	Personal information > 1,000,000 / Sensitive personal information > 10,000	Important Data	Personal information / Important Data
Specific scenarios*	Exemption (number)	Exemption (scenarios)			
The data collected and generated in the course of international trade, cross-border transportation, academic cooperation, multinational production, manufacturing and marketing, etc., without any personal information or important data		Exemption (other)			
"Personal Information Transit"					
Where a data processor within the pilot free trade zone provides any data outside the Negative List to an overseas recipient					
Other scenarios, such as data trading, telemedicine, cross-border e-commerce and financial settlement		Standard Contract/Certification	Security Assessment		

https://www.zhonglunwende.com/index.php/Index/show/catid/15/id/933.html

C. Relevant Cases

- ***(2022)粤0192民初6486号* — First judicial judgment published by the court regarding disputes over cross-border transmission of personal information after the introduction of the Personal Information Protection Law.**
  - Jurisdiction issue.
  - The court held that since Gao Company is a foreign legal entity, this case falls under a foreign-related case. According to Art 3.2 of the *PIPL*, the personal information processing conduct involved in this case falls under the category of "for the purpose of providing products or services to natural persons located within China“. <u>*Additionally, all parties in the court proceedings consented to the application of Chinese law to handle this case*</u>. Therefore, laws such as the *PIPL* were ultimately applied to adjudicate this case without further detailed discussion about this issue.
- ***Wang v. A Consulting Company and an International Hotel Company - Dispute over the Protection of Personal Information* — One of the Top Ten Typical Cases of Cross-border Data Disputes Released by the Guangzhou Internet Court**
  - About legality review of cross-border processing of personal information.
  - Transfer to different countries → Whether it necessary to fulfill the contract → whether need separate consent.

V.
Emerging Technologies and Data Privacy Updates

New Challenges

- Public Surveillance:
  - Balancing security vs. privacy (e.g., Hangzhou’s "City Brain" project)
  - Regulations on Network Data Security Management 《網路資料安全管理條例》
- Artificial Intelligences:
  - Interim Measures for the Management of Generative AI Services 《生成式人工智慧服務管理暫行辦法》 (2023, by seven departments of the State Council): Requiring separate consent for AI training data

- More Emerging Issues:
  - Unsecured Data Storage and Doxxing
  - Algorithmic Transparency: No clear PIPL guidance on explainability
  - Less Regulated Personal Information Profiling and “Sha Shu” (殺熟, “killing frequent users”)
- And more …

Thank You!