

# China's Personal Information Protection Law and Key Implications for Businesses

15 February 2022



香港信託人公會  
Hong Kong Trustees' Association

## **Barbara Li (CIPP/E)**

Head of Data, TMT and FinTech

Head of Corporate

Rui Bai Law Firm 瑞柏律師事務所

Ex-Vice Chair of Cybersecurity WG and Construction

WG of the EU Chamber of Commerce in China

## **Chiang Ling Li**

Partner

Head of Intellectual Property

Tiang & Partners



**Barbara Li (CIPP/E)**  
**Head of Data/TMT/FinTech**  
**Head of Corporate**  
+86 (10) 8540 4686  
barbara.xb.li@ruibailaw.com

Barbara Li is the Head of Corporate of Rui Bai Law Firm based in Beijing and also leads the Data, TMT and FinTech practices of our firm. With almost three-decades' solid experience working at the Beijing and London offices of leading international law firms as well as in-house role, Barbara brings a wealth of enormous expertise in advising international companies, financial institutions and Chinese businesses on doing business in China and globally. She focuses her practice on foreign direct investment, M&As, joint ventures and strategic alliances in a wide range of industries including high-tech, telecom, energy, infrastructure, automotive and high-end manufacturing. She also counsels Chinese companies on their outbound strategies and infrastructure projects.

Barbara has a particular interest in TMT and FinTech sectors, with extensive experience advising international and Chinese companies, financial institutions, tech companies and PE funds on structuring investment, achieving data and cybersecurity compliance and managing risks related to digital transformation and deployment of emerging technologies such as AI, big data, cloud and blockchain. She is well recognized as an expert in this field in the China market and is described as "having extensive experience in complex TMT regulatory issues" by Legal 500. Barbara is widely recognized in Corporate, M&A, TMT and FinTech categories and is ranked as a leading individual by various legal directories including Chambers, Legal 500, Asian Legal Business (ALB), IFLR1000 and WhichLawyer. She won the China Top TMT Lawyer Award 2020 ranked by Asian Legal Business.

Benefiting from her in-house experience, Barbara works closely with the industry and she is frequently invited to write and speak at international and regional professional and industry conferences and events to share her insights. She served as the ex-vice chair of the Cybersecurity Sub-Working Group and the Construction Working Group of the EU Chamber of Commerce in China for several years.

Barbara is dual-qualified in England & Wales and China. She obtained her LLM degrees from both King's College, University of London and the China University of Law and Political Science, where she got her LLB degree as well. She completed the CPE and LPC courses in London for pursuing her UK bar qualification.

Barbara is a native Chinese speaker and has proficiency in writing and speaking English.

“ **Rui Bai Law Firm – Tier 2 in Other Notable Firms In Beijing**  
*Legal 500, 2020*  
**Rui Bai Law Firm – Leading firm in Data Protection and TMT**  
*Legal 500, 2021* ”

“ **Barbara Li – Highly regarded practitioner**  
*IFLR, 2011-2021*  
**Barbara Li – Leading Individual in TMT**  
*Chambers 2020-2021* ”

“ **Barbara Li – China 15 Top TMT Lawyers**  
*Asia Legal Business, 2020*  
**Barbara Li – Leading Individual in TMT / FinTech**  
*Legal 500, 2020-2021* ”

**Barbara Li served as Vice-Chair of the Cybersecurity and Construction Sub-Working Groups of the EU Chamber of Commerce for several years**

# Content



**China's data law, cross data transfer and key implications**

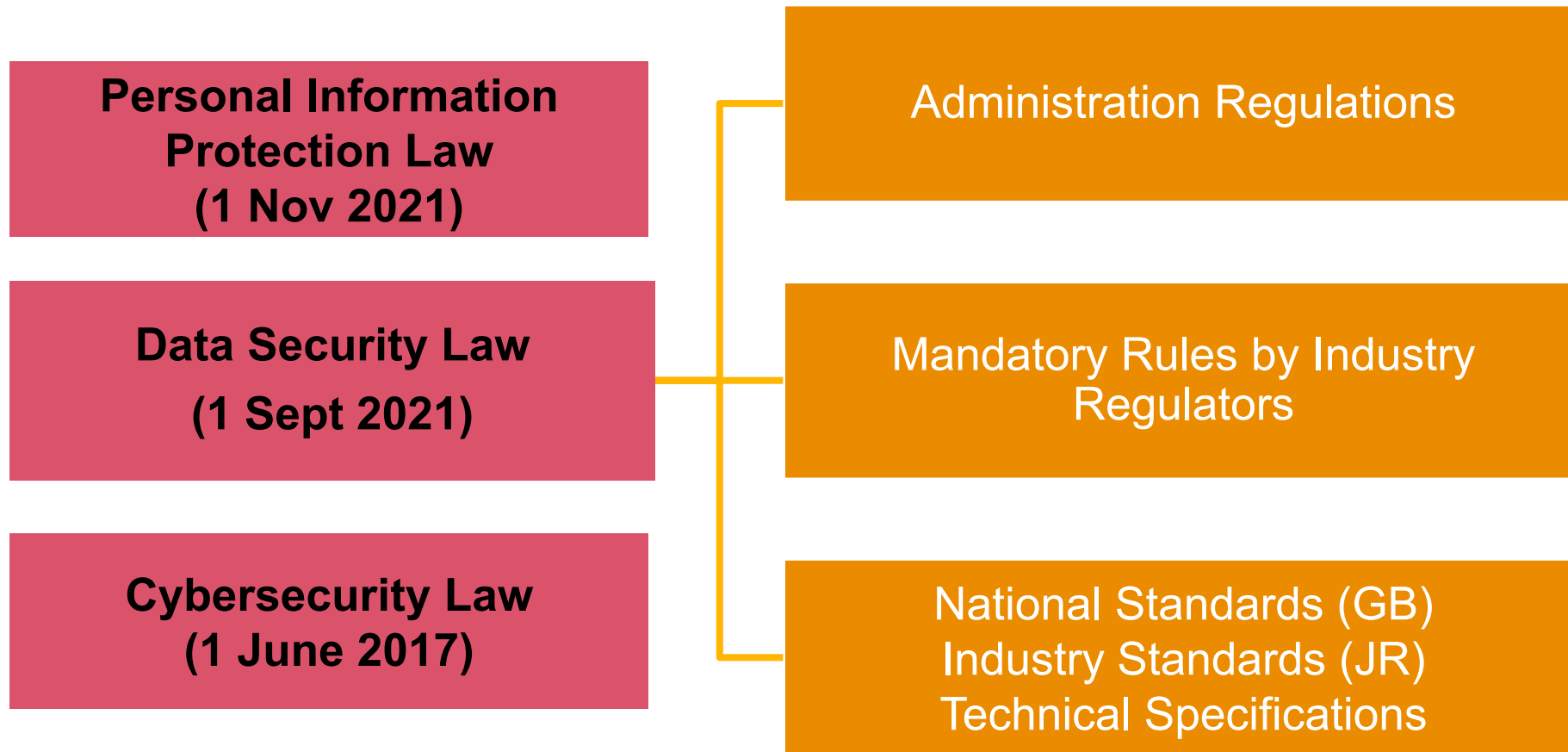


**Legal obligations, rights and liabilities**



**What to do next**

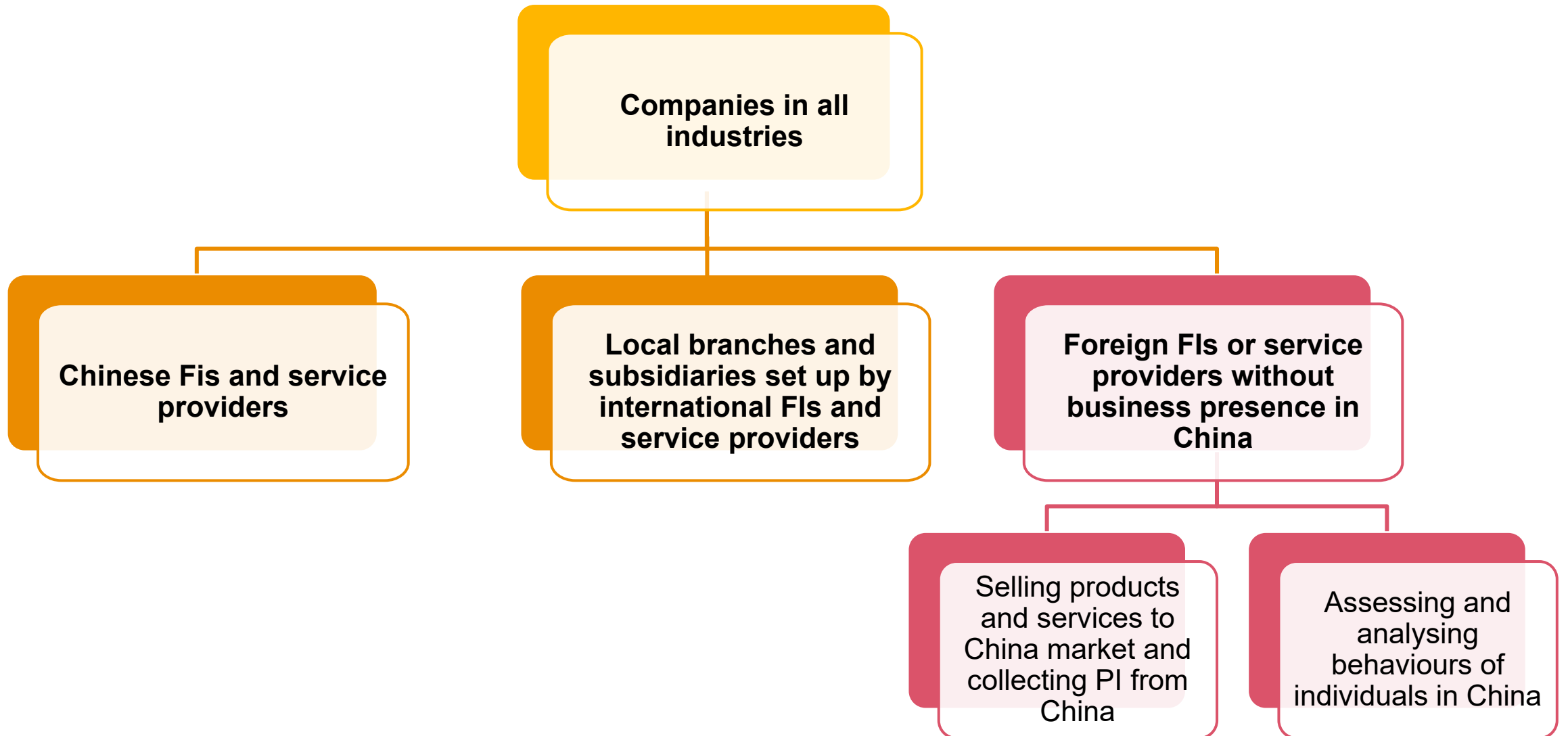
# China Data Legal Regime



# Personal Information Protection Law (PIPL)



# Who Are Covered?



# How is PI Defined?

- **Wide range**

- Any kind of information
- Related to an identified or identifiable natural person
- Sensitive PI: financial, health, biometric, PI of children <14yrs, etc.;
  - Wider scope than GDPR
  - Stricter compliance requirements



# What Activities Are Covered?

**Collection**

**Use**

**Transmission**

**Disclosure**



**Processing**

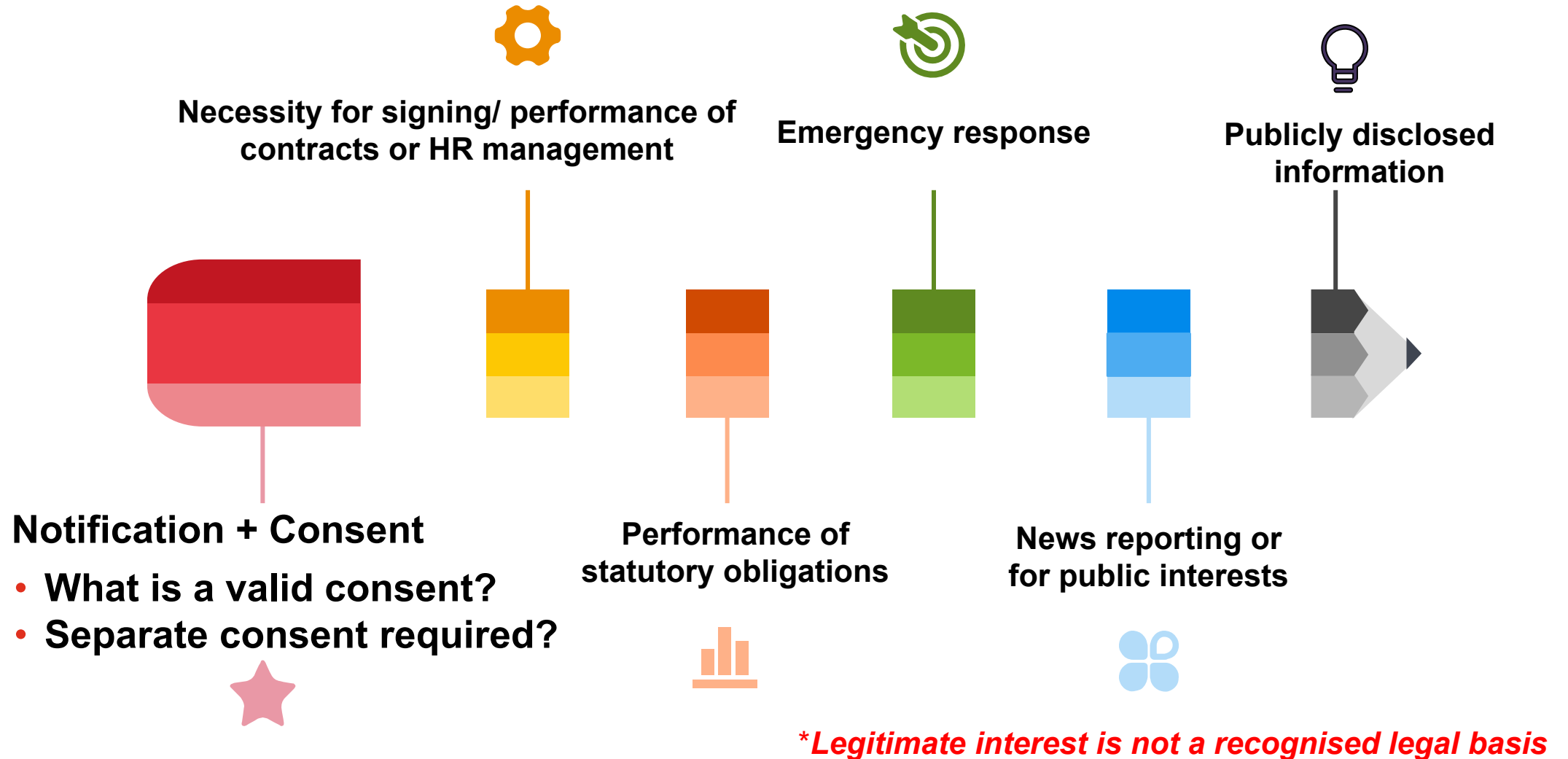
**Storage**

**Provision**

**Deletion /  
Destruction**

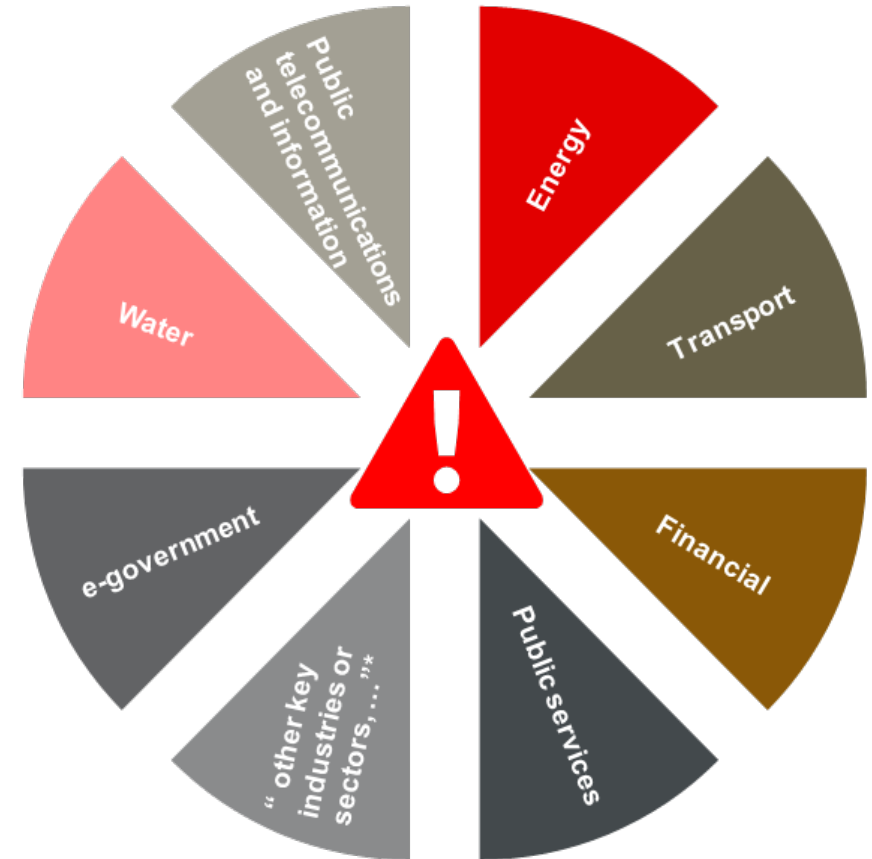


# Legal Principles and Basis – Legality, Necessity, Fairness, Transparency and Minimisation



# Data Localisation - High Risk for Specific Industries

- Critical Information Infrastructure (CII):
  - **Financial**, energy, water, public utilities, telecom and information services, transportation, e-government AND “OTHER KEY INDUSTRIES”
- **Personal Data** and **Important Data** collected/generated during business operation in China should be stored in China
- Cross-border transfer of data is only allowed on the ground of necessary and has passed security assessment



\*“other key industries or sectors, which can seriously harm national security or public interest, if destroyed or tampered with or if data is leaked”

# Cross-Border Data Transfer of Personal Information

**Cross-border data transfer by CII Operators and Non-CII operators processing size of data prescribed by authorities**

- Security assessment by government



- Security assessment by authorities
- Security certification by qualified 3rd party institutions
- Standard contract with overseas recipients
- Other mechanism allowed by laws

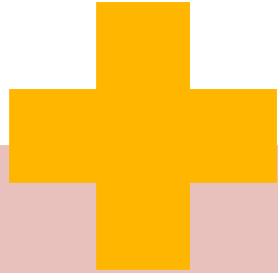
**Cross-border data transfer by non-CII operators**



**In each case:**

- Transfer to foreign judicial and enforcement authorities prohibited unless approved by Chinese authorities.
- Proper notification, separate consent and data protection impact assessment are required.

# Cross-Border Transfer of Important Data



Cross-border transfer of **Important Data** by CII operators subject to security assessment



Cross-border transfer of **Important Data** by non-CII operators subject to regulations to be issued

In each case, cross-border transfer of Important Data to foreign judicial and enforcement authorities prohibited unless approved by Chinese authorities

# More Cross-Border Transfer Requirements to Come

- **Draft Guideline for Identifying Important Data (Sept 2021)**
- **Draft Measures on Security Assessment of Cross-Border Data Transfer (issued 29 Oct 2021 by CAC)**
- **Draft Administrative Regulation on Network Data Security (issued 14 Nov 2021 by CAC)**
  - Clarities on important data
  - Lower threshold to trigger security assessment for cross-border data transfer
    - ❑ All important data
    - ❑ Data processors handling 1 million users
    - ❑ Personal information of 100k individuals
    - ❑ Sensitive personal information of 10k individuals
  - Cybersecurity review may be triggered
    - ❑ IPO outside China
    - ❑ M&A, spin-off, restructuring by large internet platform operators
- **Draft Financial Data Security Assessment Specifications (issued 26 Nov 2021 by PBOC)**
  - Financial data generated in China shall in principle be stored locally, unless permitted by laws/regs
  - Security control and procedures for cross-border data transfer

# Key Implications for Businesses

## *GDPR Compliant ≠ PIPL Compliant*

- Compliance review for business model
  - ❖ Impact assessment
  - ❖ Compliance actions and risk management

- Expanded scope and enhanced compliance requirements for cross-border data transfer



- High risk exposure for financial industry

- Enhanced compliance requirements (appointment of DPO, encryption, data breach response, training, etc)

# Contact– Chiang Ling Li



**Chiang Ling Li**  
Partner  
Head of Intellectual  
Property  
Tiang & Partners

---

## Contact

+852 2833 4938

chiang.ling.li@  
tiangandpartners.com

## Profile

---

Chiang Ling Li's practice has focused on China intellectual property law since 1994. She has been in the forefront of the law, leading successful litigation involving patents, trade secrets, copyright, unfair competition, 3-D marks and well-known marks, as well as successfully pursuing criminal enforcement of IP infringement in China. Her depth of experience has also taken her to handle projects in the realms of blockchains, NFTs and metaverse as well as projects in the traditional and digital spheres.

Chiang works closely with industry organizations lobbying for legal reforms, including those concerning patent linkage and data exclusivity, and has been appointed an arbitrator by CIETAC, HKIAC, ADNDRC, and the WIPO Arbitration and Mediation Center.

Chiang is author of *China Executive Report: Intellectual Property*, the China IP chapters of LexisNexis's *Intellectual Property Rights*, the "Anticounterfeiting and Enforcement" chapter in *China's Participation in the WTO*, and the China chapters in *PLC Cross-border Life Sciences* (2007-2012 editions), *Trade Secrets Throughout the World Treatise*, *Patents Throughout the World*, and *Designs and Utility Models Throughout the World*. She is also author of many articles on China IP and pharmaceutical law and practice.

Chiang was among the "A-List" of the top 100 lawyers for China (*China Business Law Journal*). She is also a PLC recommended lawyer in all three categories of life sciences: intellectual property, corporate and commercial (China), and corporate and commercial. Chiang also has been recognized by *The International Who's Who of Life Sciences Lawyers*, *World Trademark Review (WTR 1000)*, *Chambers Asia-Pacific* and *Chambers Global*, *The International Who's Who of Life Sciences Lawyers*, *The International Who's Who of Business Lawyers*, *IAM 1000 — The World's Leading Patent Professionals*, *WTR 1000 — The World's Leading Trademark Professionals*, and *IAM Licensing 250: The World's Leading Patent and Technology Licensing Practitioners*.

## Areas of expertise

---

- Intellectual Property
- Technology
- Global IP disputes
- Health Care & Life Sciences

# Key Requirements for Data Controller

## 1. Sensitive personal information (biometrics, religious belief, special identity, healthcare information, financial accounts, geolocation, and information of minors under 14):

- separate consent required;
- individual must be informed of necessity of processing the information and its impact; and
- consent from a parent or guardian + separate personal information processing policy, in case of a minor under 14



# Key Requirements for Data Controller (cont'd)

## 2. Personal information reaching prescribed volume

- data protection officer

## 3. Relevant foreign companies without a presence in China

- special agencies or appoint representatives in China

# Key Requirements for Data Controller (cont'd)

## 4. Impact assessment and 3 years' record retention

- Sensitive personal information
- Use personal information for automated decision making
- Entrust personal information processing to others
- Cross-border data transfer
- Data disclosure
- Data transmission to other data processors

### Impact assessment standard

- Whether the processing purposes and methods, among others, are legitimate, justified, and necessary
- Impact on personal rights and interests as well as security risks
- Whether the protection measures are legitimate, effective, and appropriate (for the level of risks)

# Key Requirements for Data Controller (cont'd)

## 5. Minimum Retained

Personal data must be collected or retained for the **minimum period for the specific purpose**, and must be **deleted or anonymized** thereafter

## 6. Security and Data Protection

Organizations need to establish **data security and protection capability** and implement relevant security controls against data leakage

## 7. Consent

**User consent** to process data must be freely given and for specific purposes

Customers must be informed of their **right to withdraw their consent**

**Separate consents** needed for processing sensitive personal information, subcontracting, cross-border transfer, etc.

## 8. Breach Notification

Organizations must **notify CAC** of data breaches

**Data subjects** need to be notified unless remedial measures taken would effectively preempt harms

## 9. Third Party Processors

When engaging a third party to process personal information, must conduct a **security assessment, supervise the third party, & enter into proper contracts** to ensure sufficient security measures are in place.

## 10. Contingency Plan

Organizations must have a **contingency plan** for security incidents and conduct **emergency drills**

# Key Requirements for Data Controller (cont'd)

## 11. Automated Decision Making

No differential treatment  
Right to **explanation**  
Convenient to **refuse**

## 12. Facial Recognition Technology

No **commercial application** unless proper consent (Separate Consent)

## 13. Foreign Investigation/Litigation

**Government approval** needed

## 14. Important Internet Platform/Large User Base/Complicated Business

**Supervisory board** composing of external members  
Publishing reports for **public supervision**

## 15. M&A/Spin-off, /Dissolution/Bankruptcy

**Notice** to individuals

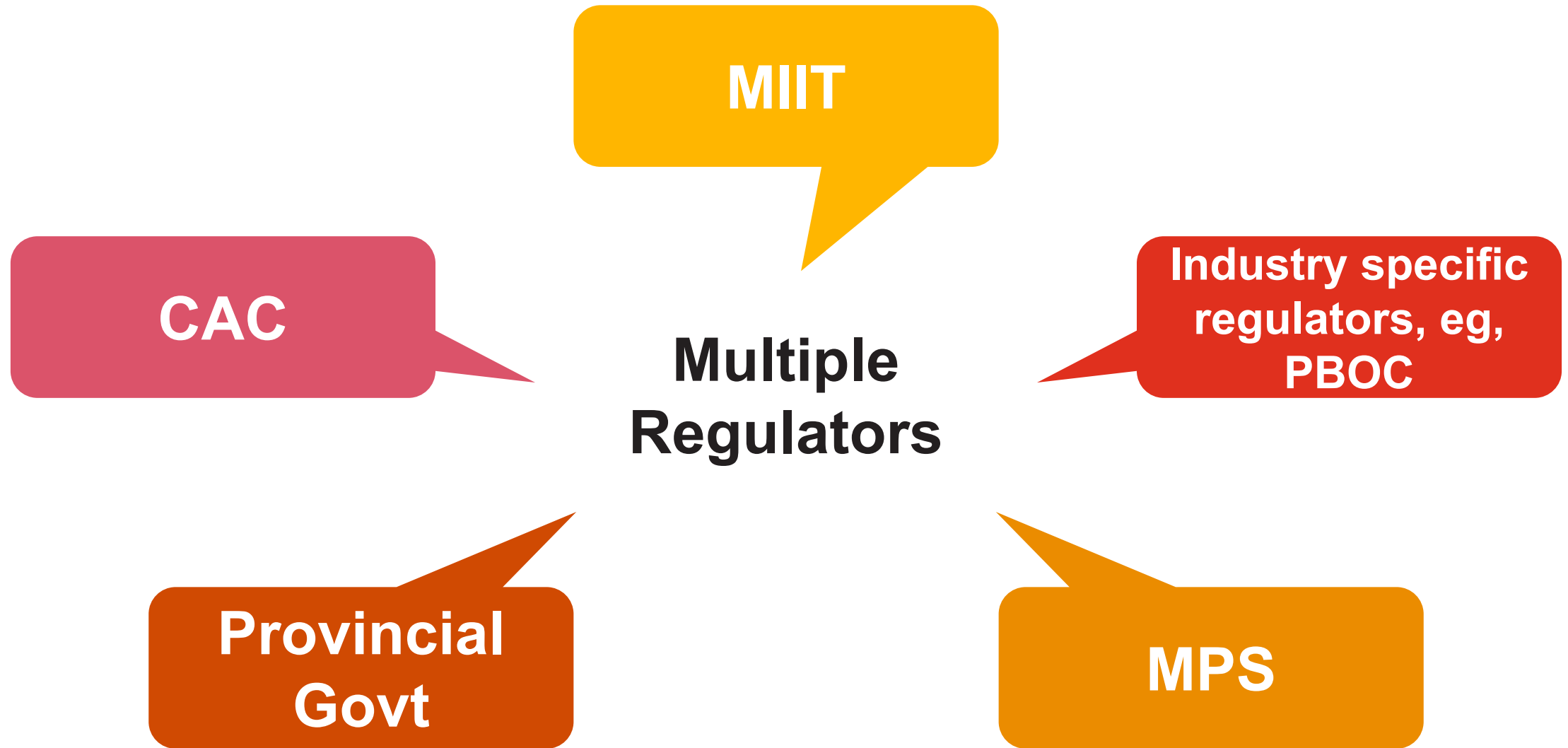
# Key Data Subjects Rights

- Access, amend, copy, transfer, delete, explain privacy policy, withdraw consent, not be subjected to automated decision making, complain, etc. rights
- For next of kin's own interests
- Prompt handling requests + convenient mechanism + explanation for non-compliance

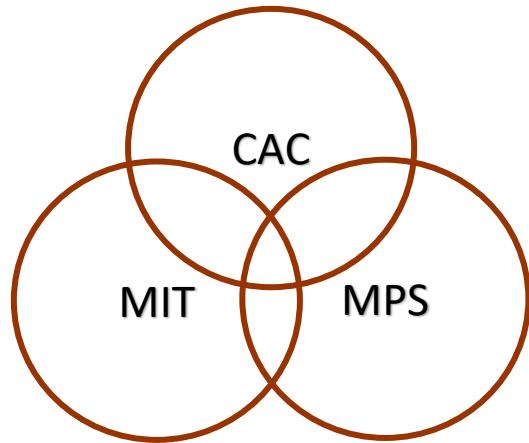
# Liabilities

- confiscation of income
- fine up to RMB 50 million or 5% of turnover of the previous year
- business suspension
- revocation of business licenses
- Violations recorded into the “credit files”
- Individuals fined up to RMB 1 million + blacklisting
- Damages (reverse burden of proof)
- Criminal prosecution

# Who are the regulators?



# Trend of Enforcement



**Regular and frequent enforcement:** Cases emerged in all regions and industry sectors

**Multi-layered enforcement:** Enforcement actions by sectors, by industries and by levels

**Key sectors focused:** Special campaigns in various key sectors

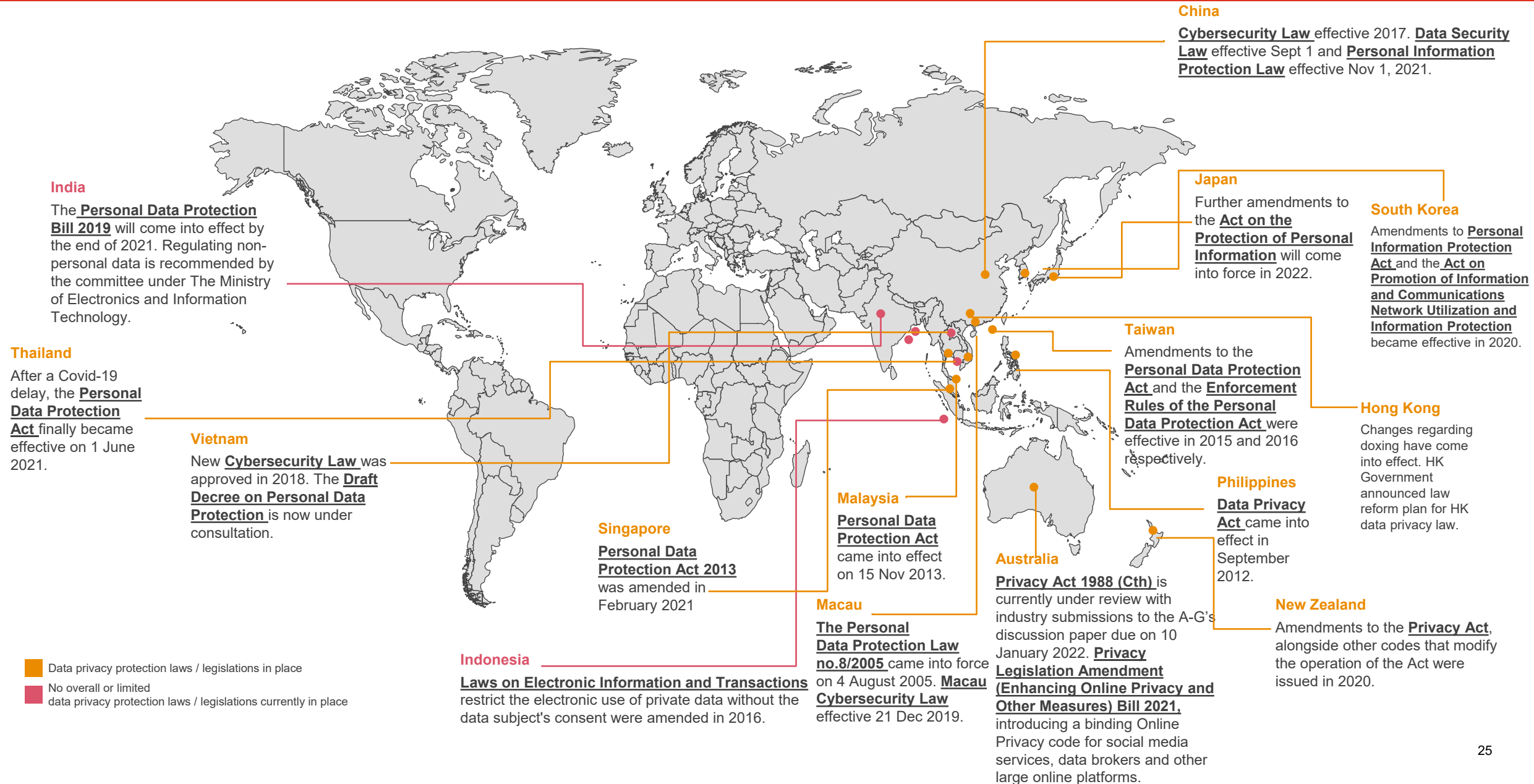
**Diversified forms of inspections:** Both on-site and remote inspections

**Nationwide publicity:** increased awareness in cybersecurity





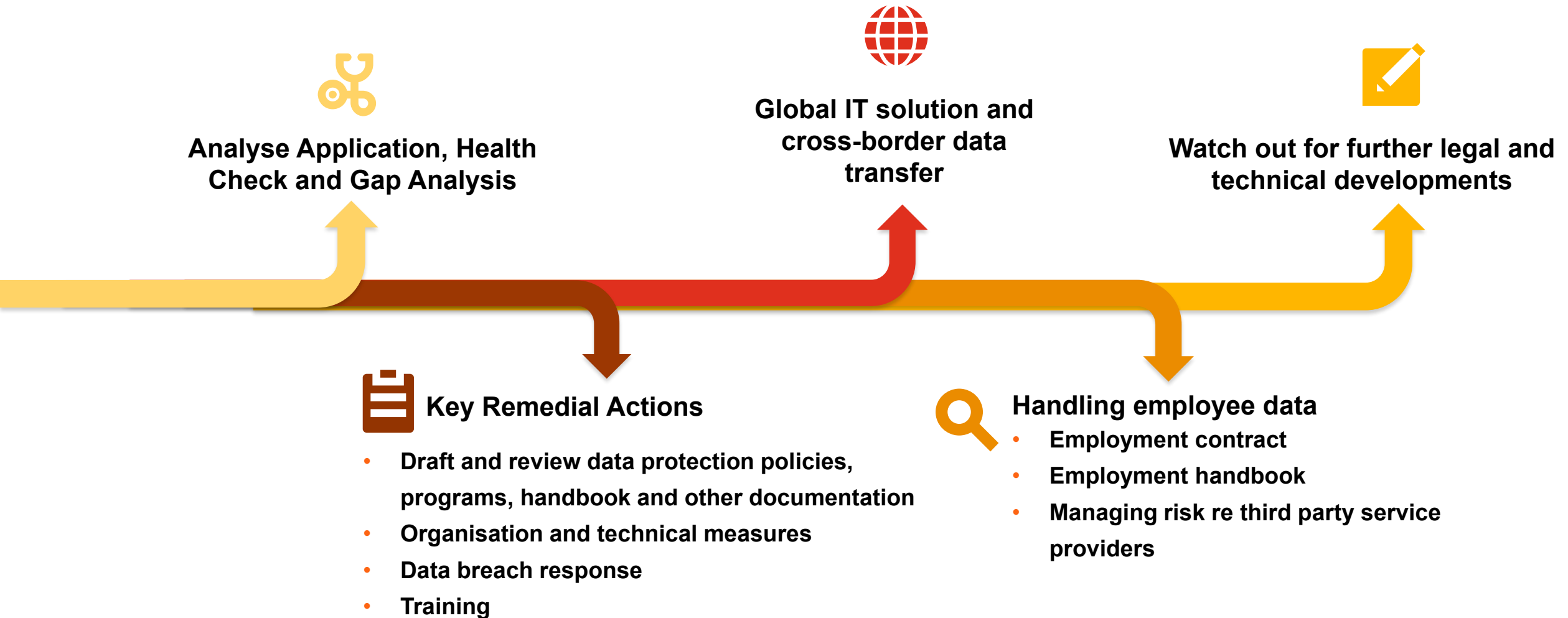
# Asia Pacific Cyber & Data Developments



# Time Is Running Out!



# Compliance Actions!





### **Barbara Li**

Head of Data/TMT/FinTech

Head of Corporate

CIPP/E

**Rui Bai Law Firm**

**Beijing**

**Ex-Vice Chair of Cybersecurity  
Working Group of EU Chamber  
of Commerce**

---

Contact

+86 (10) 8540 4686

barbara.xb.li@ruibailaw.com

### **WeChat**



### **LinkedIn**



## **Publications**

---

- [Release of the Draft Measures on Security Assessment of Cross-border Data Transfer](#)
- [China's Supreme Court specifies rules for trials of facial recognition cases](#)
- [China's First Personal Information Protection Law is about to take effect – are you ready?](#)
- [China Lawmakers Passed the Data Security Law](#)
- [China adopts new rules to further regulate e-Commerce](#)
- [China: Cybersecurity and privacy enforcement](#)
- [China - Enforcement and Breach](#)
- [Cybersecurity review of network products and services in China](#)
- [Navigating China's Cybersecurity Regulatory Maze](#)
- [IAPP Exclusion Livestreaming discussion with Barbara Li: China's new data Privacy Law: PIPL](#)
- [IAPP Exclusive Interview with Barbara Li: Privacy Around the Globe: China](#)

Q&A



# Thank you !

[www.ruibailaw.com](http://www.ruibailaw.com)

The information contained in this presentation is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of professional advice or service by Rui Bai Law Firm. Rui Bai Law Firm has no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual Rui Bai Law Firm contact or your other advisers.

The materials contained in this presentation were assembled in 2021 and were based on the law enforceable and information available at that time.

© 2021 Rui Bai Law Firm. All rights reserved.