Implementation of the PIPL and the Business Impacts

Barbara Li, CIPP/E
Partner, Beijing
IAPP Advisory Board Member
Vice chair of Cybersecurity Sub-WG of EU Chamber of Commerce in China

ReedSmith
Driving progress
through partnership

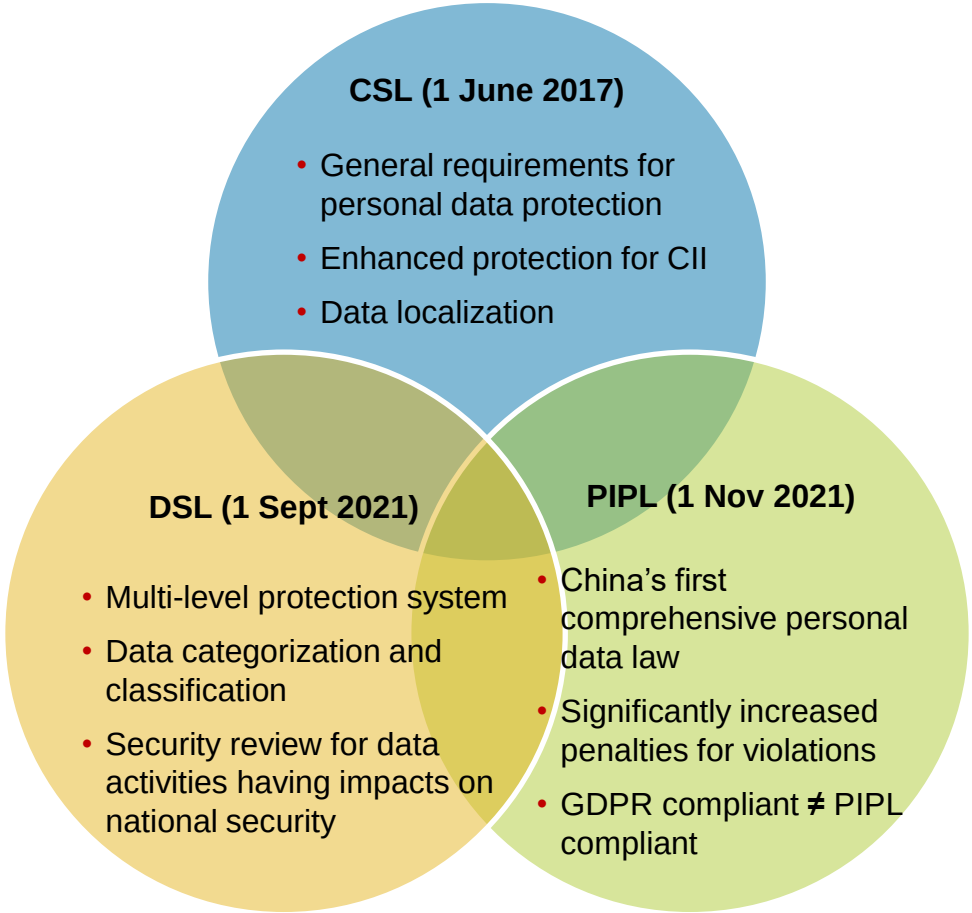
List of Content

- **Implementation of the PIPL**
- **Legal liability and enforcement updates**
- **Major impacts for businesses and individuals**
- **Practical steps for compliance and risk management**

Implementation of the PIPL

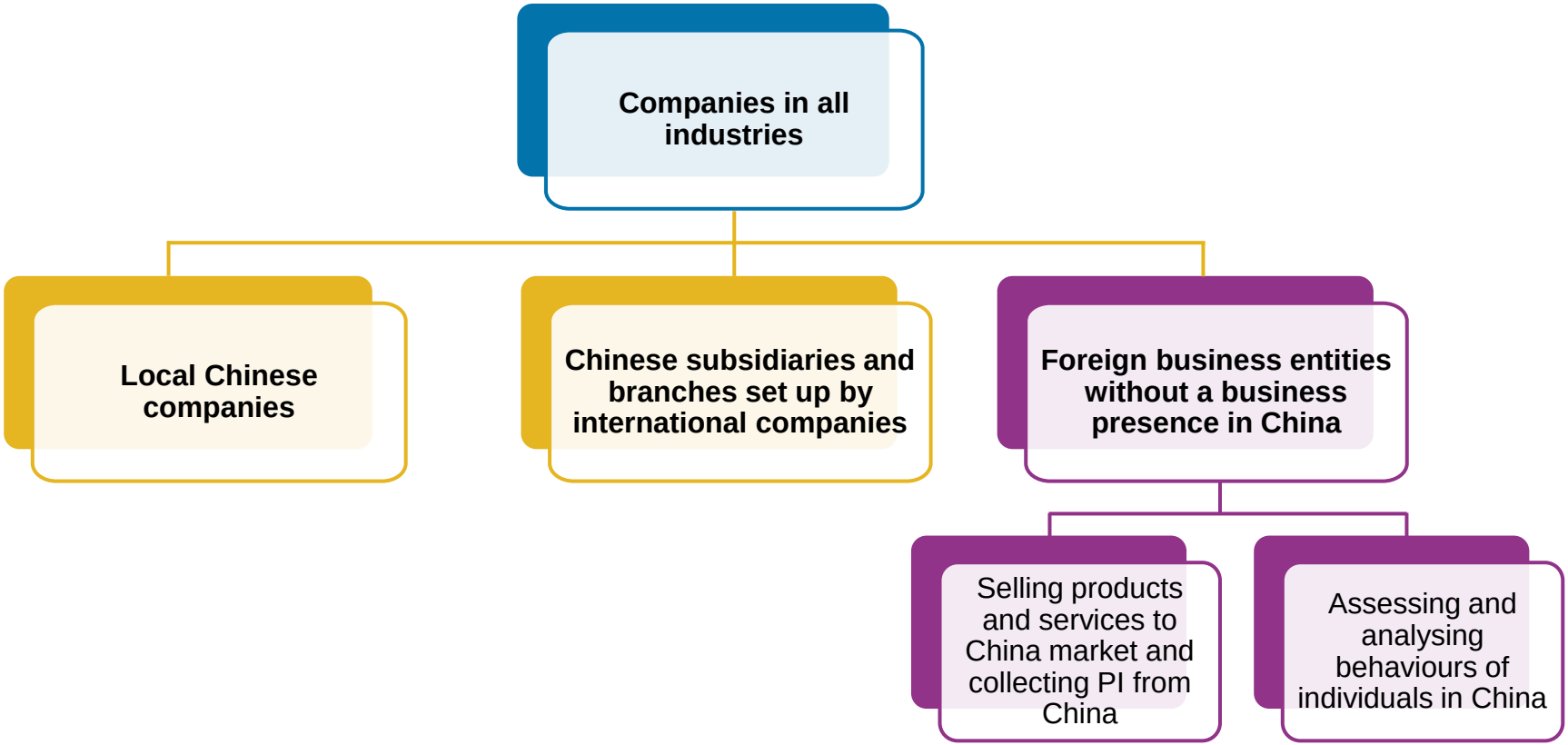
China Data Law Regime

- **"Three Pillers"**
  - Cybersecurity Law
  - Data Security Law
  - Personal Information Protection Law
- **Other national laws**
- **Administrative regulations**
- **Industry rules**
- **National specifications**
- **Judicial interpretations**



Personal Information Protection Law of China (PIPL)

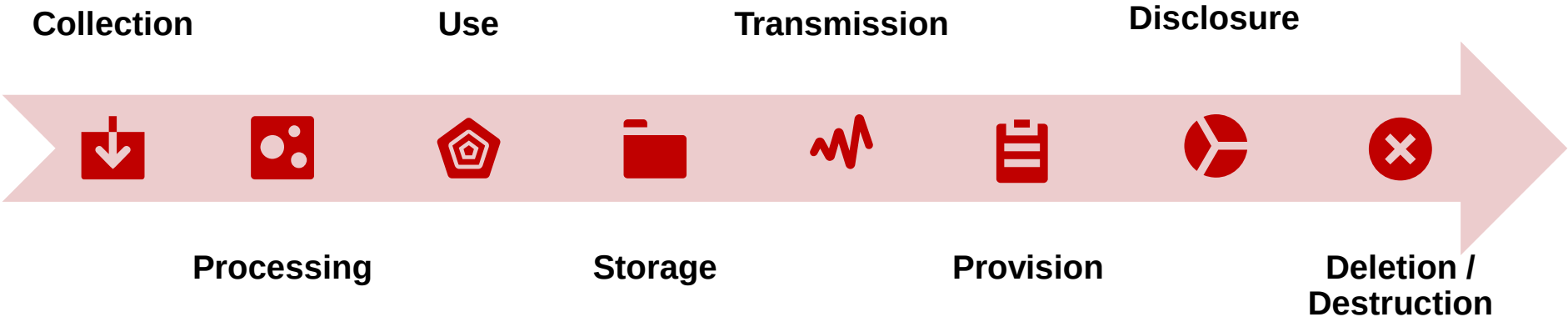
Who Are Covered?



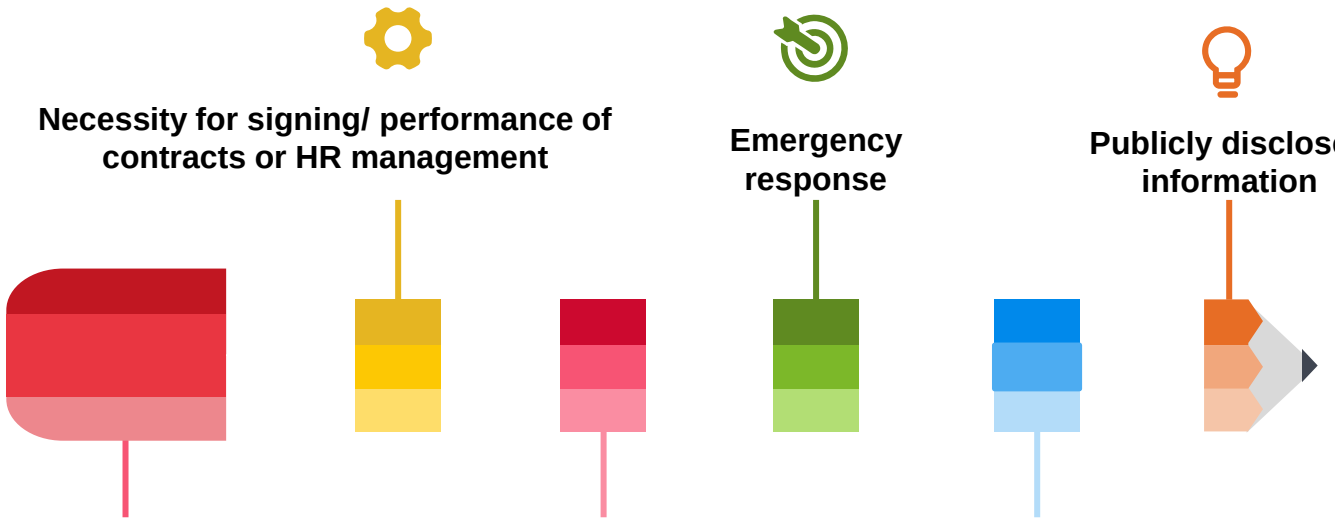
How is PI Defined?

- 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?



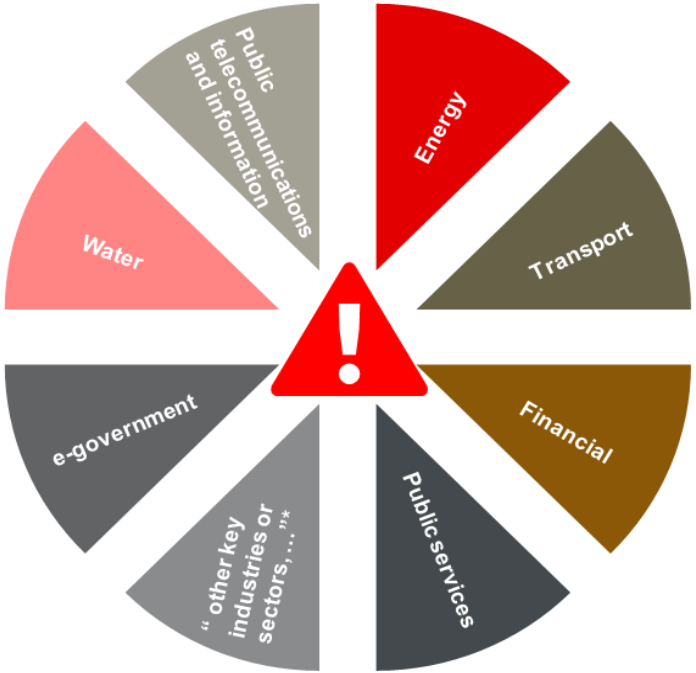
Legal Principles and Basis – Legality, Appropriateness, Necessity, Fairness, Transparency and Minimisation



*Legitimate interest is not a recognised legal basis

CIIOs and Data Localisation

- 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

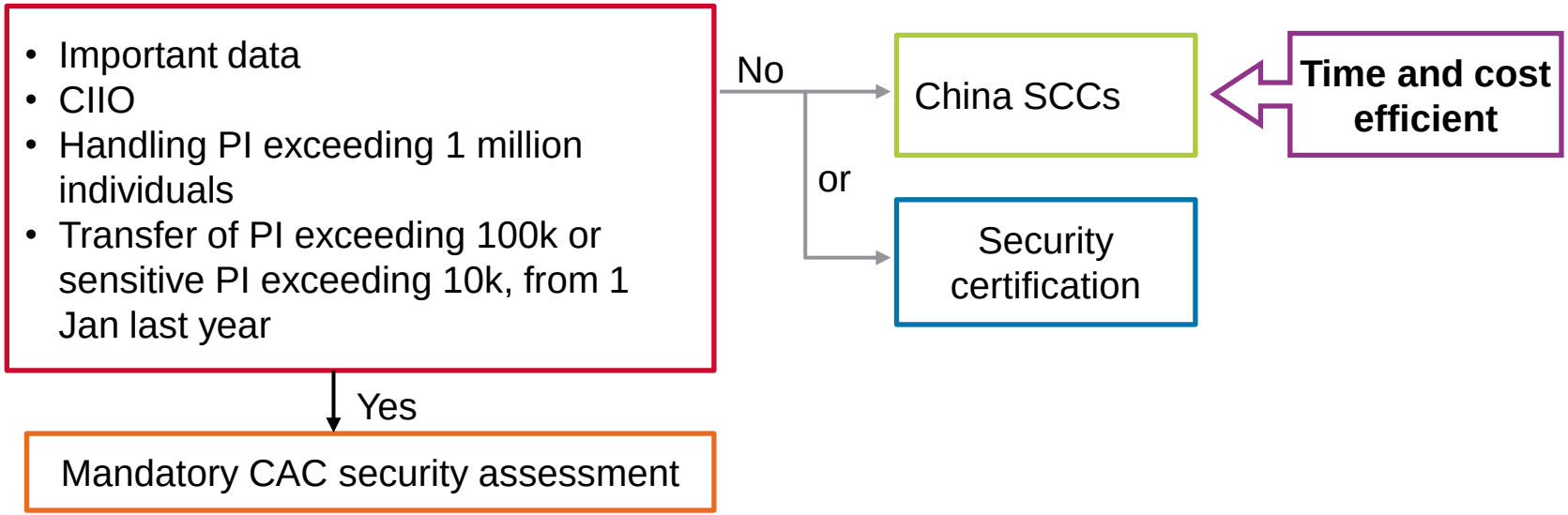


*“other key industries or sectors, which can seriously harm national security or public interest, if destroyed or tampered with or if data is leaked”

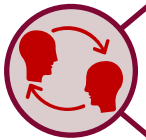
Cross-Border Data Transfer Mechanism

- Three mechanisms fully established

Which CBDT Mechanism to Choose?



Security Assessment - Documents, Procedure and Timeline



Self-assessment report (govt template w/out change, comprehensive info expected)

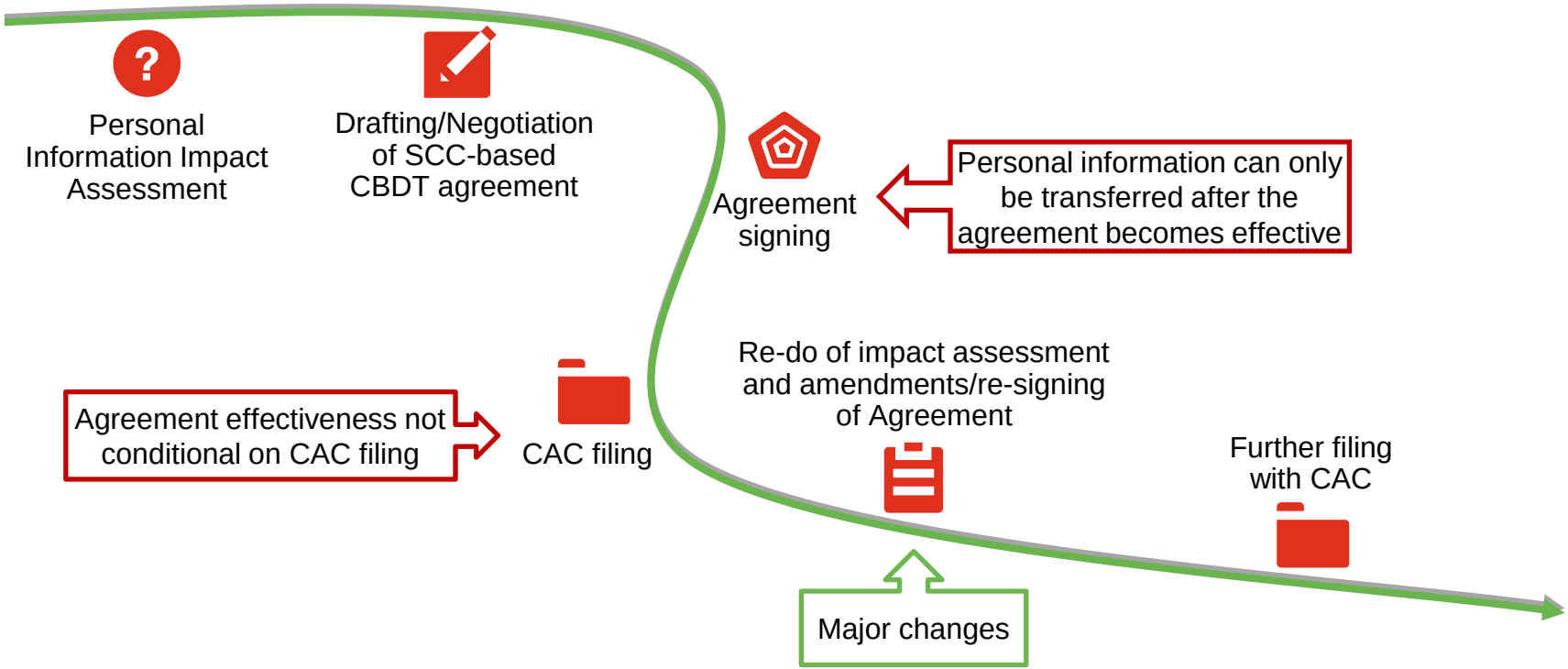
Cross-border data transfer agreement or legally binding document

Submission to provincial CAC and final review by central CAC (2-4 months expected)

Grace-period of 28 Feb expired, what to do now?

Hundreds of formal submissions to provincial CACs including MNCs and Chinese companies across sectors, esp automotive, aviation, banking, insurance, e-commerce, pharma, healthcare, retailing, tech, telecom, industrial automation, consumer brands, etc

Chinese SCCs (effective 1 June 2023)



Chinese SCCs – Easy to Use?

- SCC terms lift the compliance bar
- Comprehensive information to be collected from both China and foreign data recipients for impact assessment
- Challenges to synchronize China SCCs with global agreement adopted by MNCs
  - Different contract model
  - Lack of flexibilities on contractual terms
  - Governing law
  - Dispute resolution
- Effective on 1 June with grace-period until 30 Nov, enough time to be compliant?

Legal liability and enforcement updates

2

Legal Liabilities and Penalties

RMB 50m or 5% of last year's turnover

Business suspension, cancellation of permit, revocation of illegal gains, degrading of social credit

Personal liability for senior executives and RMB1m fine

Litigation and whistle-blowing

Criminal liability

Enforcement

- Industry focus: health, medical, financial, telecom, e-commerce, consumer brands, transportation
- Significant penalties – USD1b fines + sanctions on senior executives
- Mobile Apps
  - Non-compliant privacy policy, excessive collection of PI, difficulty in de-register, forced reactivation
  - Thousands of Apps caught, order for rectification within given time, removal from app stores
- Active investigations in Beijing, Shanghai, Shenzhen, Zhejiang and Sichuan
- Stronger privacy awareness from the public
  - Litigations and consumer claims
  - Employee claims
- Vigorous enforcement anticipated with new data enforcement regulations to come into force on 1 June 2023 and significant increase of penalties in draft Revised Amendments to the CSL

Major impacts for businesses and individuals

3

Key Implications for Businesses and Individuals

GDPR Compliant ≠ PIPL Compliant

- Impacts on business model, products and services and need for compliance analysis
- IT infrastructure deployment and contracting structure

- Data compliance to be integrated into day-to-day business operations
- Non-compliance can result in hefty penalties and other significant legal, business and reputational risks

- Data subject's rights
- In response to whistle-blowing and claims by individuals

- Call to action for complying with CBDT legal requirements and other compliance steps
- Make good faith efforts and document them

Practical steps for compliance and risk management

4

What Pitfalls to Avoid

"This can't be right. Does this apply to us?"

"This targets Chinese Tech giants. We don't need to bother. "

"The legal requirements are not clear and some implementing rules are not finalized. Let's just wait and see."

"We are GDPR compliant. GDPR is stricter than PIPL, so we are safe."

"We need to store all data in China!"

What Practical Steps to Take

Compliance health-check

- Data mapping
- Compliance gap analysis
- Strategy aligned with business objectives and priorities
- Special attention to regulated sectors and high risk aspects

Draft/Update privacy documentation

- Privacy policy
- Consent
- Employment contract and handbook
- DPAs

Cross-border data transfer

- Determine appropriate mechanism for cross-border data transfer
- Take immediate compliance action for security assessment, PIPIA, SCC contract terms and other required docs
- Allow sufficient lead time for information collection and coordination, documents preparation, response to enquiries from authorities

Data breach response

- Notification to data subjects and regulators
- Prepare data breach pack
- Data breach drill
- Insurance

Ongoing compliance and risk management

- Build up compliance system
- Learn from enforcement lessons
- Training
- Keep close watch on regulatory, legal and technical developments

Contact Us

Barbara Li
Partner, Reed Smith Beijing Office
IAPP Advisory Board Member
Vice chair of Cybersecurity Sub-WG of EU Chamber of Commerce in China
Admitted in England & Wales / China Bar Qualification Holder

E: bli@reedsmith.com
T: +86 10 6535 9531

Linkedin WeChat

- Chinese SCCs come out – are you ready? – Reed Smith
- Data transfers in the EU, UK, and China - Tech Law Talks – Reed Smith
- China adopts new guidelines for certification of cross-border data transfers – Reed Smith
- China issues new Implementation Rules for Personal Information Certification – Reed Smith
- Blockchain and data protection – An FAQ guide – Reed Smith
- Cross-border data transfer mechanism in China and practical steps to take – Reed Smith
- China MLPS 2.0 – Baseline requirements and practical takeaways for businesses - Data Guidance
- IAPP Linkedin Live - Chinese SCCs Are Here - Are You Ready?
- A look at what's in China's new SCCs - IAPP
- Top-5 Operational Impacts of China's PIPL: Part 2 Obligations and Rights - IAPP
- What to know about China's new cross-border data transfer security assessment guidelines - IAPP
- IAPP Asia-Pacific Dashboard Digests
- IAPP Global legislative predictions 2023 (China Part)
- The Importance of Being a PIPL Pleaser: Update and Predictions on China's Data Protection Law One Year In - Cybersecurity Law Report