DEZAN SHIRA & ASSOCIATES
Your Partner for Growth in Asia

China PIPL Best Practices: Refining Your Data Security and Compliance

August 10, 2022

About Us

1992	Dezan Shira’s establishment
400+	Our **team** of legal, tax, accounting, business intelligence and audit professionals
3,000+	Multinational **clients** that have already chosen us
80+	**Countries** served by our professional services
35	**Offices** in China, Hong Kong, India, Vietnam, Singapore, Indonesia and Mongolia; Liaison offices in Italy, the United States and Germany, and Asian Alliance offices in Malaysia, the Philippines, Thailand, Bangladesh, Japan, South Korea and Taiwan.

DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Today’s Speakers

Thomas Zhang
Partner
Shenzhen office
thomas.zhang@dezshira.com

Guilherme Campos
Manager
International Business Advisory
Shenzhen office

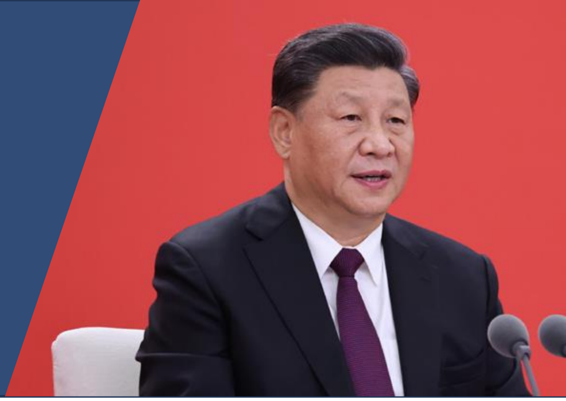
guilherme.campos@dezshira.com

DEZAN SHIRA & ASSOCIATES
Your Partner for Growth in Asia

Key Points

Section 1	**Intro**
Section 2	**Overview of The Cyber Security Legal Framework**
Section 3	**Key Considerations to be Compliant with PIPL**
Section 4	**Practical Cases Concerning the PIPL**
Section 5	**Outlook for Future Development of China’s Data Protection Landscape**

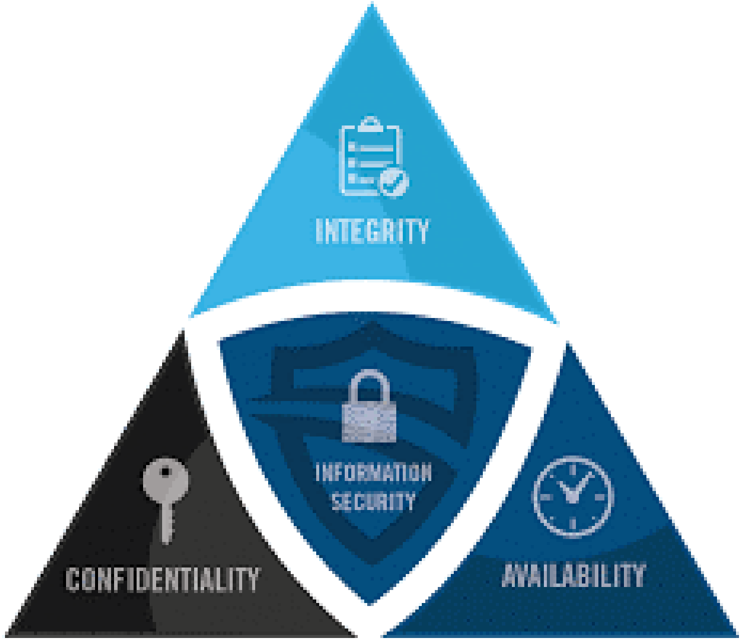
> *“The Development of the Internet has posed new challenges to national security, sovereignty and development interests.”*
>
> *“Without Cyber Security there is no National Security”*



Privacy is much broader than ***security***

Privacy and security are deeply ***intertwined***

Security control measures are beneficial to privacy, though not enough



Privacy and Personal Data

- **Identity**
  - Identified individual
  - Pseudonym
  - Anonymity

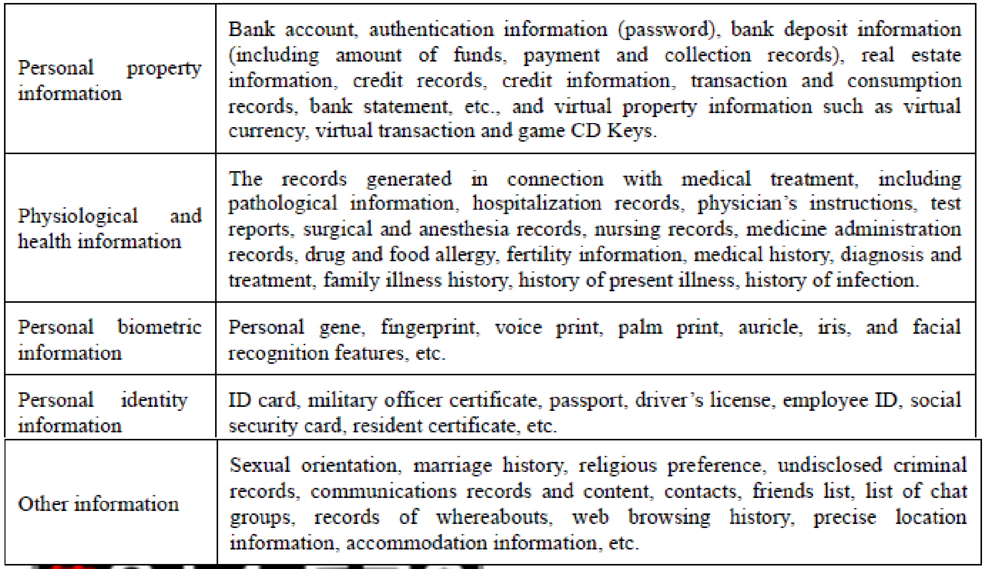
- **Types of Personal Data**
  - Direct vs indirect personal data
  - First-hand vs 3rd party personal data
  - Sensitive personal data

- **Privacy and Privacy Management**

中华人
PEOPLE'S REP
外国人永久
FOREIGN PERMANE
本证是持证人在中国境内居留的身份证
医疗、交通、住宿、通信、工作、税收和社
事务时单独使用。
THIS DOCUMENT SERVES AS AN IDENTITY CARD FOR THE
CHINA AND CAN BE USED INDEPENDENTLY AS LAWFUL PROO
RELATING TO FINANCE, EDUCATION, HEALTH CARE, TRAVEL, ACC
EMPLOYMENT, TAX, SOCIAL SECURITY, PROPERTY REGISTRATI

CSL

Table B.1 Examples of sensitive personal information

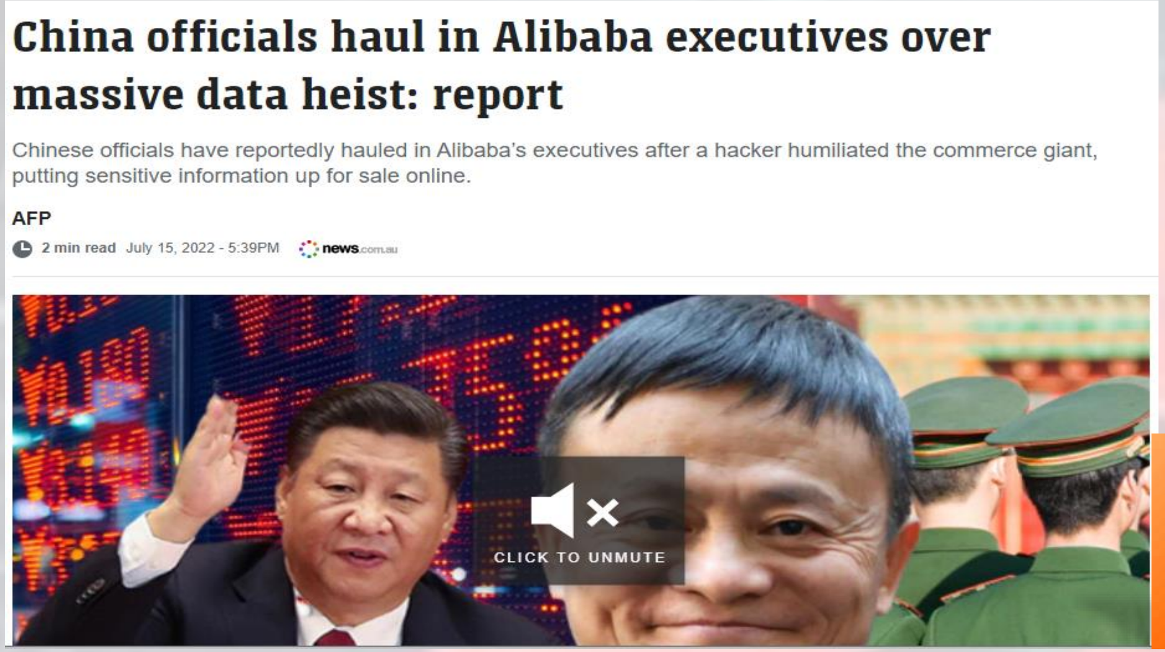


Personal property information	Bank account, authentication information (password), bank deposit information (including amount of funds, payment and collection records), real estate information, credit records, credit information, transaction and consumption records, bank statement, etc., and virtual property information such as virtual currency, virtual transaction and game CD Keys.
Physiological and health information	The records generated in connection with medical treatment, including pathological information, hospitalization records, physician's instructions, test reports, surgical and anesthesia records, nursing records, medicine administration records, drug and food allergy, fertility information, medical history, diagnosis and treatment, family illness history, history of present illness, history of infection.
Personal biometric information	Personal gene, fingerprint, voice print, palm print, auricle, iris, and facial recognition features, etc.
Personal identity information	ID card, military officer certificate, passport, driver's license, employee ID, social security card, resident certificate, etc.
Other information	Sexual orientation, marriage history, religious preference, undisclosed criminal records, communications records and content, contacts, friends list, list of chat groups, records of whereabouts, web browsing history, precise location information, accommodation information, etc.

GDPR

- ✓ data revealing racial or ethnic origin
- ✓ data revealing political opinions
- ✓ data revealing religious or philosophical beliefs
- ✓ data revealing trade union membership
- ✓ genetic data
- ✓ biometric data processed for the purpose of uniquely identifying a natural person
- ✓ data concerning health
- ✓ data concerning a natural person's sex life or sexual orientation

The Impact of the Regulations on Companies



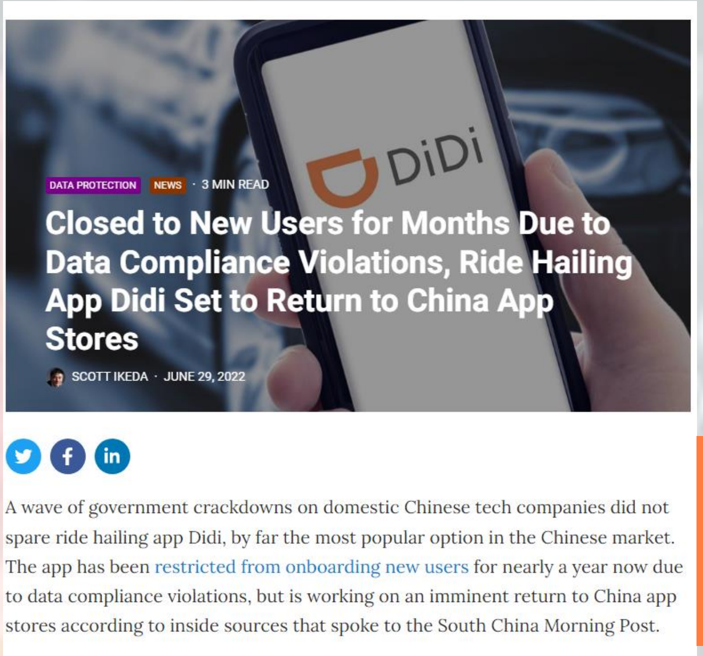
China officials haul in Alibaba executives over massive data heist: report

Chinese officials have reportedly hauled in Alibaba's executives after a hacker humiliated the commerce giant, putting sensitive information up for sale online.

AFP

2 min read July 15, 2022 - 5:39PM news.com.au

Alibaba.com



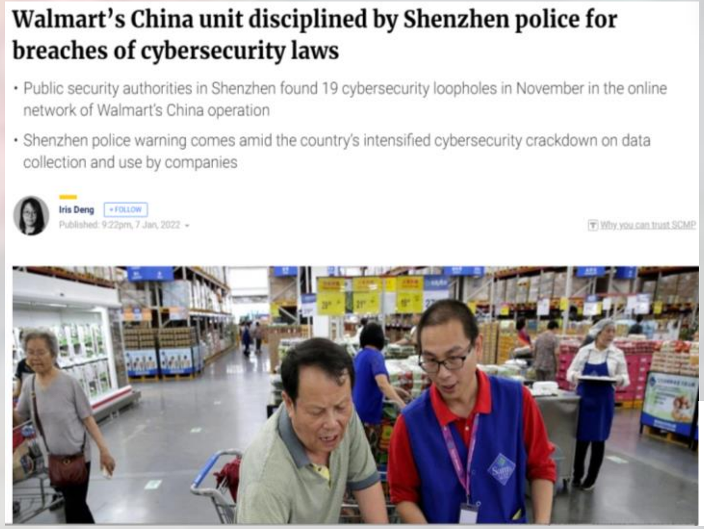
DATA PROTECTION NEWS · 3 MIN READ

Closed to New Users for Months Due to Data Compliance Violations, Ride Hailing App Didi Set to Return to China App Stores

SCOTT IKEDA · JUNE 29, 2022

A wave of government crackdowns on domestic Chinese tech companies did not spare ride hailing app Didi, by far the most popular option in the Chinese market. The app has been restricted from onboarding new users for nearly a year now due to data compliance violations, but is working on an imminent return to China app stores according to inside sources that spoke to the South China Morning Post.

DiDi



Walmart's China unit disciplined by Shenzhen police for breaches of cybersecurity laws

- Public security authorities in Shenzhen found 19 cybersecurity loopholes in November in the online network of Walmart's China operation
- Shenzhen police warning comes amid the country's intensified cybersecurity crackdown on data collection and use by companies

Iris Deng + FOLLOW

Published: 9:22pm, 7 Jan, 2022

Why you can trust SCMP

Walmart
Save money. Live better.

Section 2

Overview of the Cyber Security Legal Framework

Legal Framework

- **Cybersecurity Law of PRC** – effective Jun 1, 2017
  Defines how to operate and maintain a network with the purpose of ensuring Cybersecurity for national and public interest.

- **Data Security Law** – effective Sep 1, 2021
  Regulates data processing and security to guarantee and protect individuals, organizations and National interests.

- **Personal Information Protection Law** – effective Nov 1, 2021
  Protects natural persons personal information.

Regulations:

- *Provisions of the governance of the online information content ecosystem (March 2020)*
- *Cyber Security Review Measures (February 2022)*
- *Regulations on the Security and Protection of Critical Information Infrastructure (August 2021)*
- *Network Data Security Management Regulation (Exposure draft) (November 2021)*
- *Measures for the Security Assessment of Outbound Data (July 2022)*
- *Provisions on the Standard Contract for Outbound Cross-border Transfer of Personal Information (Consultation Draft) (June 2022)*
- *Administrative Provisions on Algorithm Recommendation for Internet Information Services (March 2022)*

CYBERSECURITY - Assess and Prevent – Who are you? Which steps to take?

1

Network Operator

Collects, process, exchanges and storages info

❑ Set an internal management system.
❑ Secure data and manage localization.
❑ Enhance Cybersecurity activities:
- antivirus protections
- define who oversees Cybersecurity
- dedicated technical Taskforce to actively monitors and prevent attacks

❑ Define a Cybersecurity Emergency response plan.

2

Critical Information Infrastructure Operator

Operates in critical industries (Healthcare, Energy, Nat Defense, Finance, Public Communication)

In addition to the above:

❑ Provide internal training on Cybersecurity, keep relevant records.
❑ Annual assessment of potential threats.
❑ Strict policies for cross-border data transfer and data storage.

DATA SECURITY - Data Management and Protection – the basics

01 Data classification (Personal Data, Important Data, Core National Data..)

02 Set Data Security management system

03 Provide internal training, keeping relevant records

04 Enhance technical activities in data management and protection

05 Properly manage Data Cross Border when required

06 Secure data and manage localization

PERSONAL INFORMATION PROTECTION

01 Define internal management system and procedures on Data processing, analyze potential legal implications and responsibilities within the Company.

02 Collect consent on data processing already at Recruitment stage

03 Identify a Personal Information Referent.

04 Beware of data cross border policy and regulation, Data shall be stored within PRC territory.

05 Provide internal ongoing training, keeping relevant records.

Section 3

Key Considerations to be Compliant with PIPL

Main Features of the Personal Information Protection Law (PIPL)

The processing of personal information and the concept of <u>“Consent”</u>

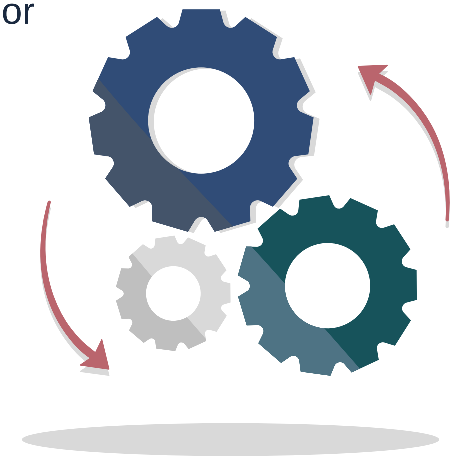
for the processing of a person (“subject”) personal information, that subject must express consent, this consent shall be , according to ***Article 14:***

- should be given by the subject and he/she must have full knowledge of what he is consenting to
- should be freely given in a voluntary and explicit manner
- should be demonstrated by a clear action of the individual (through email, signed letter or e-form, etc.)

Also...

may later **<u>be withdrawn</u>** and a subject’s <u>separate consent</u> to process their info is required when:

- sensitive personal information is processed
- the personal information is provided by the processor to another processor
- the personal information is transferred outside of China



Main Features of the Personal Information Protection Law (PIPL)

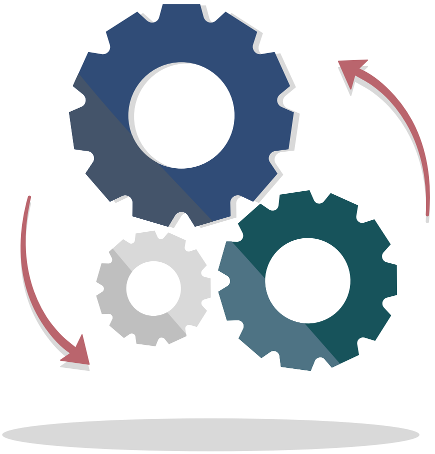
Exceptions to the consent rule:

Article 13 allows the following exceptions to the consent rule:

- necessary for the conclusion or performance of a contract or for human resources management
- necessary for statutory duties and obligations
- necessary for public health emergencies
- for news reporting and other activities concerning public interest
- disclosed by the individual himself
- other circumstances as provided by laws and regulations

And the subjects always have the right to:

- access, correct, erase , object and restrict the processing of the individual’s data
- right to data portability
- right not to be subject to automated decision making
- right to withdraw consent
- right to lodge a complaint with the regulator



Main Features of the Personal Information Protection Law (PIPL)

Obligations to safeguard personal info and legal consequences of noncompliance:

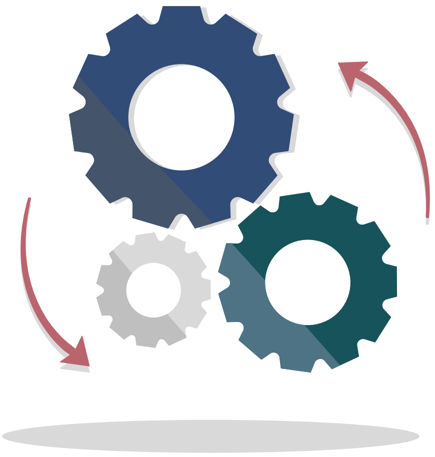
- Formulate internal management systems and operational procedures
- Implementing classified management of personal information
- Adopt corresponding technical security measures (e.g. encryption and de-identification)
- Determining operational authorizations for personal info and provide regular security education and training for operational staff.
- Formulating and implementing response plans for security incidents relating to personal info
- Conduct regular compliance audits
- Adopting other security measures as stipulated by laws and regulations

!

Punishments:

Fines up to 50 million RMB or 5% of the company's annual revenue for the prior financial year

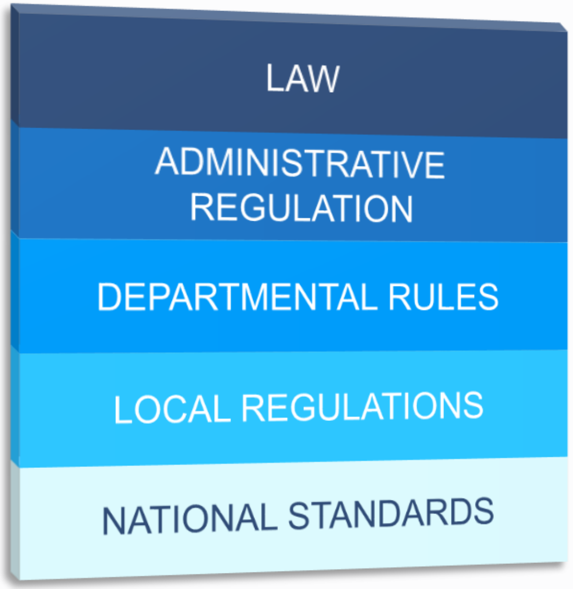
for individual punishments, subject to a fine up to 1 million RMB



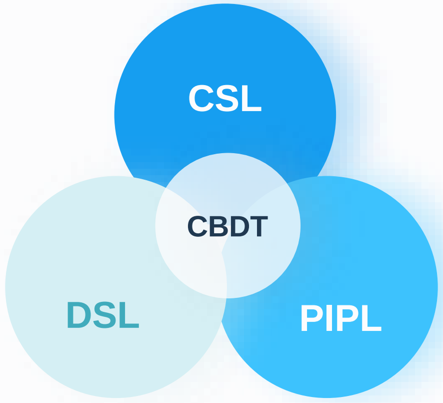
Section 4

Practical Cases Concerning the PIPL

Special Challenges of Compliance in China



Complex regulatory environment



Intertwined compliance requirements

CYBERSPACE ADMINISTRATION OF CHINA

cac.gov.cn

中华人民共和国工业和信息化部

- 国家网信办网络数据管理局
- 工信部信息通信管理局
- 工信部网络安全管理局
- 公安部网络安全保卫局
- App违法违规收集使用个人信息治理工作组
- 全国“扫黄打非”办公室
- 国家计算机病毒应急处理中心
- 国家移动互联网安全管理中心
- 各地网信办、通管局、公安局、消协…

Multiple supervisory agencies

What We Can Learn from Didi Case?

- **Huge of penalty would not be a “normal” punishment for general companies, but learn to know why Didi received the penalty would give a reference meaning to all companies for taking care own business’ compliance**

- **Illegal Facts – 16 items in 8 categories identified as per CAC**
  - Access the capture pic inside mobile illegally
  - Over-access mobile clipboard, app list of user’s mobile
  - Over-access facial recognition info, age, occupy, relationship, home and company address info of passenger
  - Over-access location info of passenger,
  - Over-access driver’s education info and don’t encrypt sensitive PI such as ID no.
  - Utilize “big data” to analyze passenger’s intention of travel, residency city and travel city info without notification
  - Request irrelevant mobile permission such as call
  - Fail to explain the purpose of 19 kinds of PI processing

Common PI Processing Scenarios and Issues

External

- Processing of general business contact info (B2B)
- Processing consumer's PI which may include sensitive PI (B2C)
- Mobile App (3rd part SDK, unnecessary access permission from mobile)
- Sharing PI to 3rd party and CBDT
- Co-handler in business partnership scenario

Internal

- HR-related activity (recruitment - CV, on-boarding, HR management) ; common issue – permanent saving of CV, staff records; collect too much PI such as employee family info; background investigation – sharing info
- Attendance (biometric info process; saving where?– be careful 3rd party attendance service such as SaaS cloud service)
- Monitoring (CCTV, email/internet access)
- Legal basis – consent (suggested) or contract (argument); separate consent

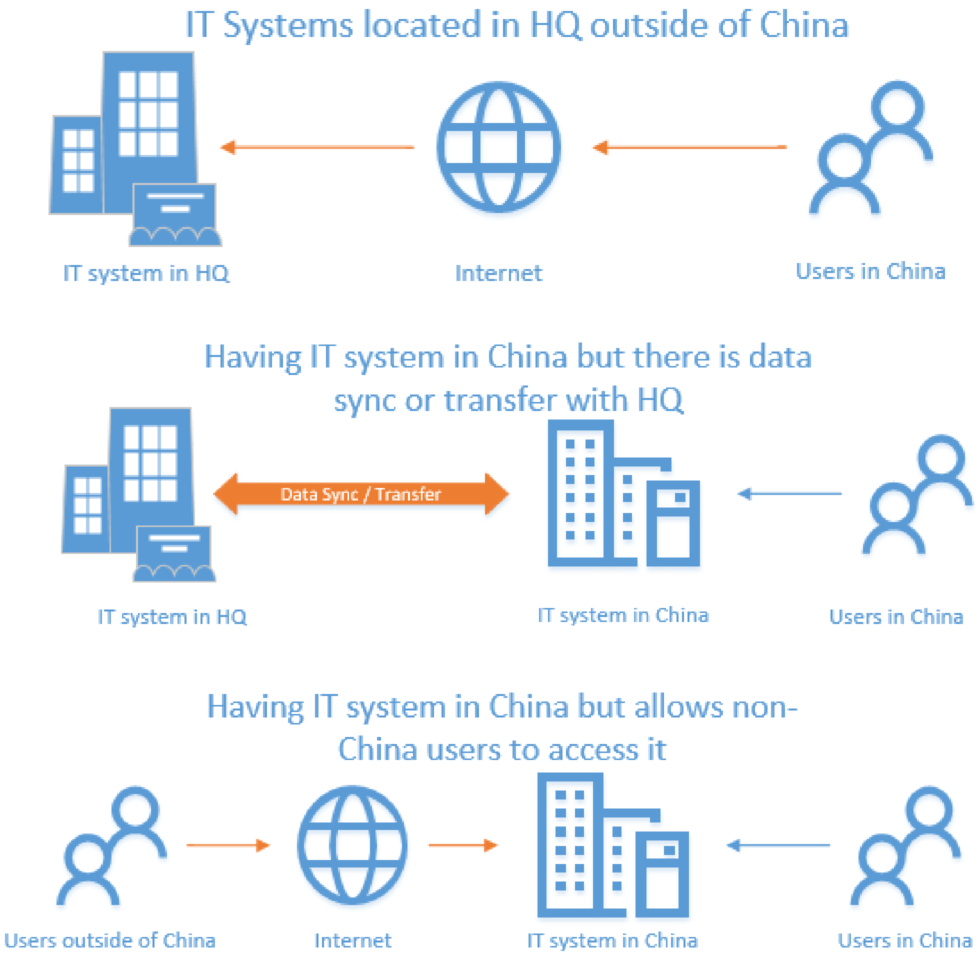
Cross-Border Data Transfer (CBDT)

Common scenarios of CBDT

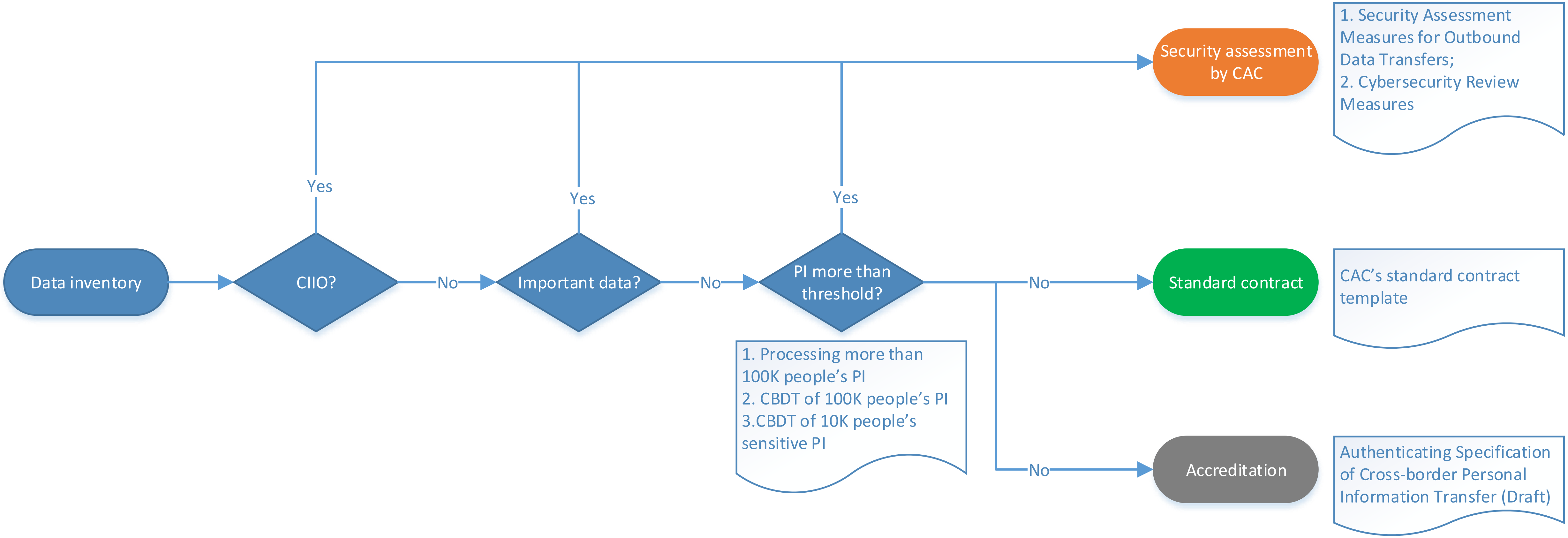
- **Data sharing for business purpose**
  - Single way (outside of China)
  - High frequency or a stable arrangement
  - Large size of data

- **Data sharing for law enforcement between countries**
  - Double way
  - Low frequency
  - Small size of specific data

CBDT for IT Pespective


IT Systems located in HQ outside of China
IT system in HQ
Internet
Users in China
Having IT system in China but there is data sync or transfer with HQ
Data Sync / Transfer
IT system in HQ
IT system in China
Users in China
Having IT system in China but allows non-China users to access it
Users outside of China
Internet
IT system in China
Users in China

Compliance Framework of CBDT



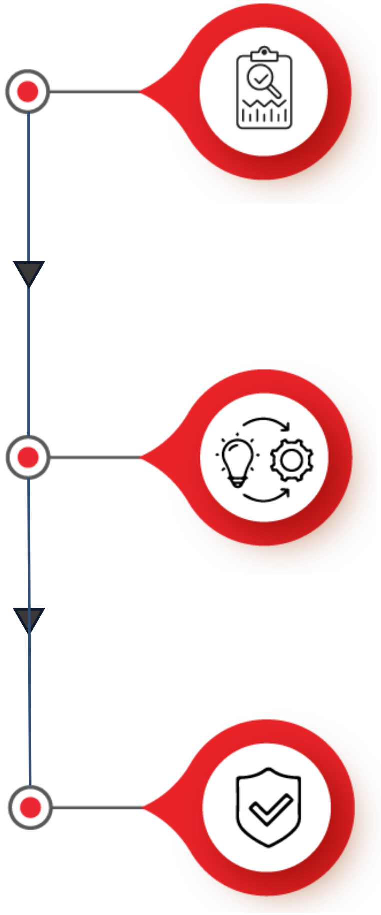
1. Processing more than 100K people's PI
2. CBDT of 100K people's PI
3.CBDT of 10K people's sensitive PI

1. Security Assessment Measures for Outbound Data Transfers;
2. Cybersecurity Review Measures

CAC's standard contract template

Authenticating Specification of Cross-border Personal Information Transfer (Draft)

Roadmap for IT Compliance



Initial Review (Phase 1)

- Understanding the nature of the business, existing IT infrastructure, and IT operations.
- Identifying the applicable laws and regulations.
- Identifying potential compliance issues.
- Suggesting action items for improvement.

Implementation (Phase 2)

- Creating a compliance action plan.
- Implementing the action plan.
- Seeking accreditation (mandatory process requested by authorities, industry standards).

Governance

- Building and maintaining the data protection management system.
- Maintaining technical and organizational control measures.
- Implementing ongoing review and improvement through the Plan-Do-Check-Action (PDCA) cycle.

Suggested Actions

Determine the strategies

- Distributed or centralized team / policy for privacy & security
- Follow localized compliance of multiple-jurisdictions respectively or follow the most stringent one to cover all jurisdictions

Organizational Actions

- Understand the importance and thinking compliance in large lens
- Equip (internal or external) resource and appoint the role with responsibility defined
- Distinguish security and privacy (PI protection)

Technical Actions

- Plan and design the proper IT infrastructure for CBDT and DSR
- Analyze existing PI processing activity with output of Data Mapping
- Perform the security protection

Case Study

EU Manufacturing Company

Main Issues

- PI processing of internal HR Management
- CBDT and security weakness

Action plan

- Keep using HQ-based IT infrastructure
- Legal documents
- Security enhancement

JOB HUNTER

Global HR Service Company

Main Issues

- Large size of sensitive PI processing
- CBDT (potential security assessment)

Action plan

- Data localization by moving servers to China
- MLPS / ICP Filing / PSB Filing

Section 5

Outlook for Future Development of China’s Data

Future Prospects

01

Key timeframe of Cross-Border Data Transfer strategy and consideration of Plan B

- Security Assessment Measures of CBDT being effective on Sep 1st of 2022
- 6 months grace period provided till to end of Feb. of 2023

02

Less uncertainty of CBDT and would be perhaps controlled more loosely due to international cooperation and usage of data as a production factor

- Clearer CBDT mechanism (PIPL / Measures for Data Export Security Assessment)
- International agreements (RCEP / CPTPP /DEPA /Digital Silk Road

03

More law enforcement activities would be expected

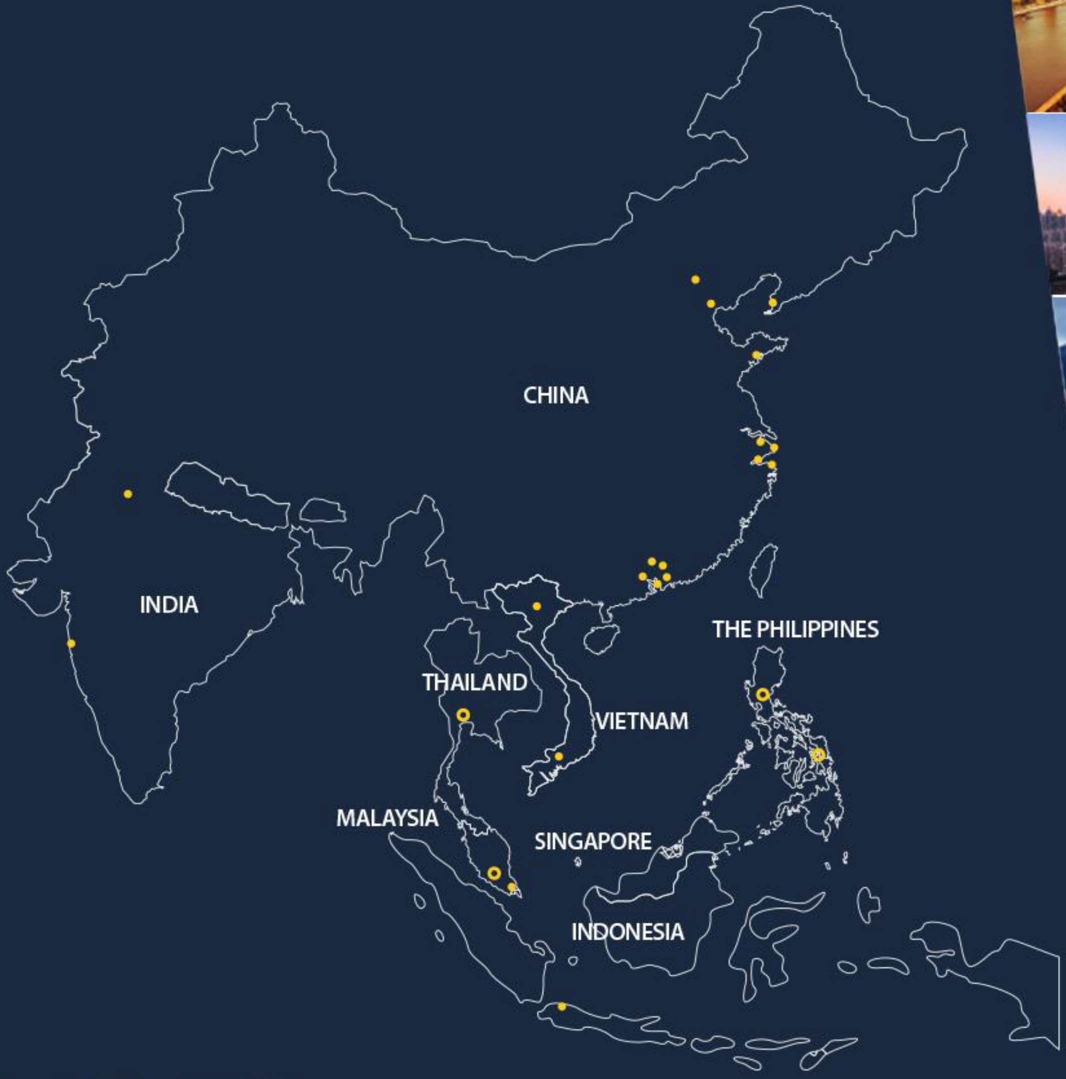
- Didi is the first case of PIPL punishment but will definitely not be the last, though the amount of penalty to Didi is not a "normal"
- Individual liability

04

Dynamic regulatory environment with provision of more supplement

- More departmental rules, local regulations
- More national standards

DEZAN SHIRA & ASSOCIATES
Your Partner for Growth in Asia



● Dezan Shira & Associates Offices
○ Dezan Shira Asian Alliance Members

Q&A

AN INTRODUCTION TO

Doing Business in China 2022

Special Focus

China's Evolving Cybersecurity and Data Protection Regime

ASIA BRIEFING
www.asiabriefing.com

Newsletter

WeChat:
DSA_China