DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

China's Personal Information Protection Law: What to Know and How to Prepare

Thomas Zhang

Nov 1st , 2021

Your Speaker Today

Thomas Zhang

IT Director

thomas.zhang@dezshira.com

Thomas has been working in the IT industry for **more than 20 years** and has rich experience on IT advisory, information security & compliance, cloud, IT infrastructure design & implementation, system administration, internal process / procedure control, and other IT related fields.

Thomas has been focusing on compliance and information security in recent years to help clients deal with the challenges caused by complex compliance requirements when doing business in China and across Asia.

Certifications and Qualifications

- **IAPP CIPT** (Certified Information Privacy Technologist)
- **EXIN DPO** (Data Protection Officer) and **ISO** (Information Security Officer),
- Member of ISACA with **CISA** (Certified Information System Auditor) certification and **CDPSE** (Certified Data Privacy Solutions Engineer) certificates
- ISC2 member with **CISSP** (Certified Information System Security Professional) and **CCSP** (Certified Cloud Security Professional) certificates

Why Focus On Personal Information (Privacy) Protection?

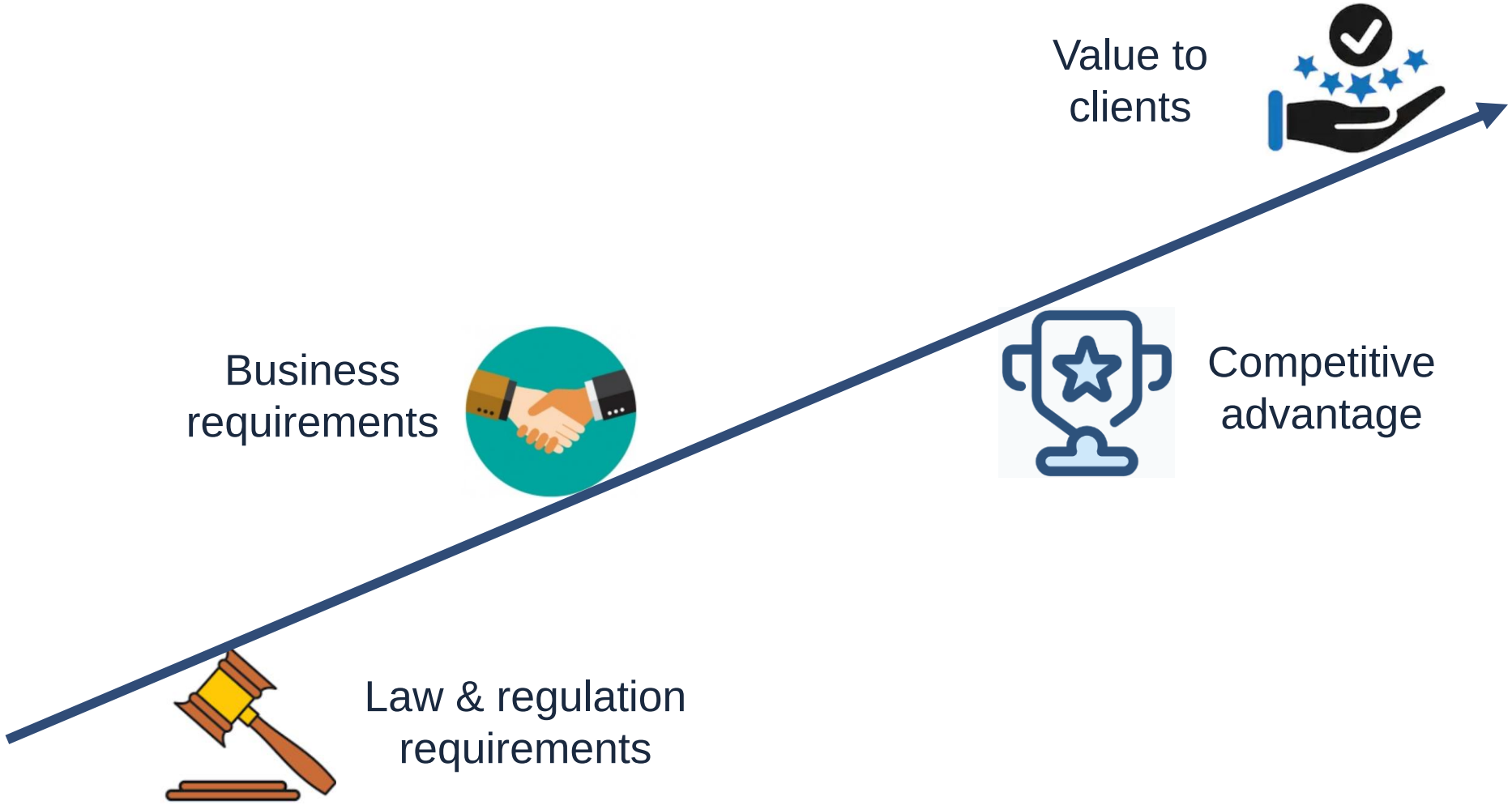


Table of Contents

Section 1

Introduction of IT Compliance in China

Birds-eye View of IT Compliance-related Laws and Regulations in China

Laws

- Criminal law
- Civil Code
- **CSL** (Cybersecurity Law, 2017)
- **DSL** (Data Security Law, 2021)
- **PIPL** (Personal Information Protection Law, 2021)

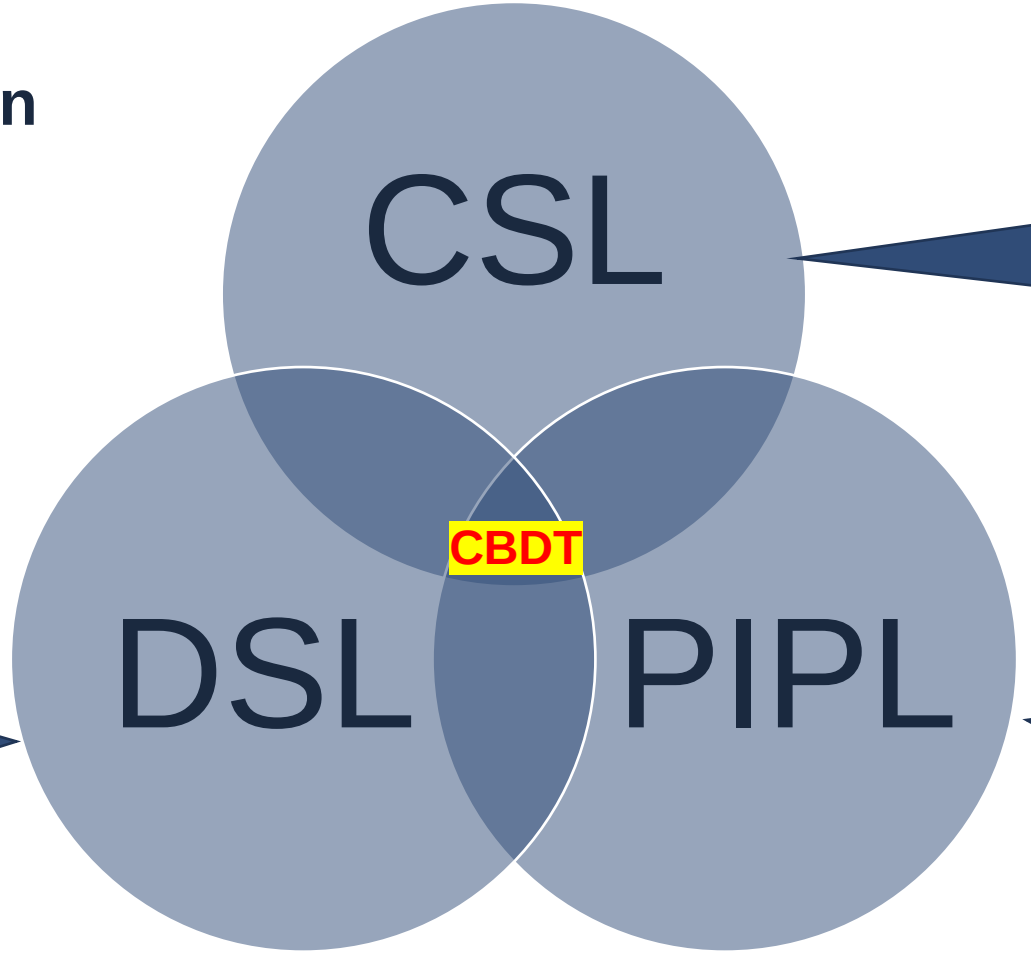
Regulations

- Internet management
- MLPS (Multi-Layer Protection Scheme)
- CII (Critical Information Infrastructure)
- Children's Personal Information
- Security Review
- Personal information cross-border transfer
- …

National Standards

- GB/T 35273-2020 (Personal info security specification)
- GB/T 39335-2020 (PIA)
- GB/T25058-2019 (MLPS implementation guide)
- GB/T 28448-2019 (MLPS requirements)
- GB/T 22239-2019 (MLPS baseline)
- GB/T 22240-2020 (MPLS classification)
- …

China's Legal Realm of Information Security and Personal Information Protection



- Effective from Jun 1st, 2017
- Focused on network security (IT Infrastructure)
- **MLPS** (Multiple Layer Protection Scheme) / **CII** (Critical Information Infrastructure)

- Effective on Sep. 1st , 2021
- Focused on data security
- Requests data classification and lifecycle management

- Effective on Nov 1st, 2021
- Focused on personal information protection
- Multiple responsibilities for Data Processors (Personal Information Handlers)

Multiple Supervisory Authorities (Data Protection Agency)

- **CAC – focused on internet content and coordination at the top level**
- **MIIT – focused on industry management**
- **MPS – focused on criminal activity and security issue**

cac.gov.cn

CYBERSPACE ADMINISTRATION OF CHINA

中华人民共和国工业和信息化部

MIIT (Ministry of Industry and Information Technology

MPS (Ministry of Public Security)

中国人民银行
THE PEOPLE'S BANK OF CHINA

中国银行保险监督管理委员会
China Banking and Insurance Regulatory Commission

中华人民共和国教育部
Ministry of Education of the People's Republic of China

- ICP Filing
- ICP License
- Mobile App
- Privacy

- PSB Filing
- MPLS
- Security breach

- Industry standard
- Pre-approval

Section 2

Key Considerations for Complying with PIPL

Extraterritorial Applicability of PIPL

Facts

- **Applicable to any processing activities of personal information within territory of China**
  - vs GDPR
- **Applicable to overseas personal information processing activities with purpose of providing products or services to natural persons in China**

Questions

- **An establishment (legal entity) in China is necessary if providing service to China?**
  - ➢ Not exactly
- **What should we do to comply with the PIPL if we intend to provide products or services in China but no legal entity in China yet?**
  - ➢ Appointment of a representative in China

Legal Justifications of Personal Information Processing

Processing based on Consent

- **Consent from individual prior to processing personal information**
- **Most widely used but the individual can withdraw the consent freely**

Processing based on a legal permission

- **Necessary for performing a contract or HR management**
- **Necessary for performing statutory duties**
- **Necessary for public health or protection of life, health, property safety of natural person**
- **Necessary for news reporting**
- **Process disclosed personal information in a reasonable scope**

Sensitive Personal Information

- **Much wider scope compared to GDPR**
- **Extra obligations**
  - Separate consent
  - PIA (Privacy Impact Assessment)
- **Common activities related to processing sensitive personal information:**
  - Payroll processing
  - HR records
  - CCTV
  - Attendance using biometric tools

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.

GB/T 35273-2020 Information security technology – Person information security specification

Cross-Border Data Transfer (CBDT)

A few questions on CBDT

- **How to define “border”?**
  - Territory is the common explanation
  - Physical location of the IT facility for processing personal information
- **Meaning of “transfer”?**
  - Data copy / transfer
  - Remote access
- **Applicable to which kind of data?**
  - Collected and processed personal information in China

Common scenarios of CBDT

Cross-Border Data Transfer (CBDT) (Cont.)

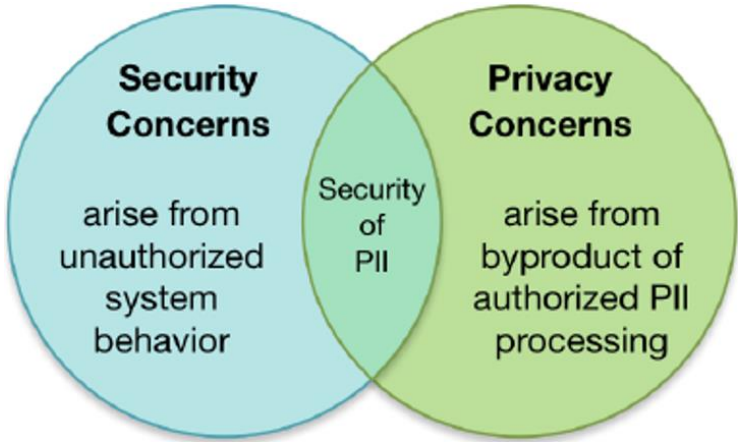
CBDT is forbidden when:

- **Processed personal information exceeds the criteria defined by CAC (PIPL)**
- **Data processed by a CII Operator (CSL)**
- **Core or Important data (DSL)**

CBDT is permitted when:

- **Passing the security review**
  - Case by case
  - vs “adequacy decision” of GDPR
- **Certified by a specialized agency**
- **Signing a CBDT contract with a standard template**
  - Template formulated by CAC
  - vs SCC / BCR of GDPR

Security and Privacy (Personal Information Protection)



Privacy ≠ Security

- Privacy and security are deeply **intertwined**
- Privacy is much **broader** than security
- Security control measures are beneficial to privacy, though **not enough**
- You can have good security without privacy if no PII processed, but you **can't have good privacy without security.**

DPIA (Data Protection Impact Assessment) / PIA (Privacy Impact Assessment)

When is a DPIA required?

- **When processing sensitive personal information**
- **When there is Cross-Border Data Transfer activity**
- **When entrusting a 3rd party to process personal information**

How to perform a DPIA?

1. Identify the need for a DPIA
2. Describe the information flows
3. Identify privacy and related risks
4. Identify and evaluate privacy solutions
5. Sign-off and record the outcomes
6. Integrate the outcomes into a project plan
7. Consult with internal and external stakeholders

Data Mapping / Data Inventory

Few questions as starting points for personal information protection:

- **Who** collects the data, in **which way**, **from whom**, and for what **purpose**?
- **Which system** is used to save personal data and in which **format**? Where is the **physical location** of the system?
- Who has **access** to the data and for what **purpose**?
- Is the data being shared with a **third party** and for what purpose, if any?

Data Mapping Record		**Created by:____**	**Input by:____**	**Date:____**	**Version:____**			
Source	**Personal Data**	**Reason**	**Handling**	**Disposal**	**Consent obtained**	**Subject is over 14**	**Sensitive personal data**	**Mission-critical data**
How was this data collected? Contact form External organization	What data are you collecting? IP address Email address Phone number	Why do you need to collect this data? CRM Processing/analytics	Explain how you will store the data, how it will be processed, and who has access to it	When will the data be disposed of?				
Contact form	Email address Phone number	CRM	Saved to CRM system for marketing event communications, only marketing team needs to access it.	After 6 months	Yes	No	No	Yes

Roadmap to Compliance

Initial Review (Phase 1)

- Understanding of business nature, existing IT infrastructure and IT operation
- Identify the applicable laws and regulations
- Identify the potential issues for compliance
- Suggestions of actions for improvement

Implementation (Phase 2)

- Create an action plan to be compliant
- Work with client and external vendor (when needed) to implement the plan
- Accreditation (Mandatory process requested by authorities, industry standard)

Governance

- Build up and maintain the personal information management system
- Maintain the technical and organization control measures
- Ongoing review and improvement with PDCA (Plan-Do-Check-Action) cycle

The **keys** of successful PIPL compliance:

- Engagement and commitment of senior management
- Joint effort and expertise of both legal and technology experts
- Appointment of a DPO (Data Protection Officer)

Q&A Session

Questions?

Feel free to contact me after the webinar with further questions or for a consultation.

Thomas Zhang

IT Director

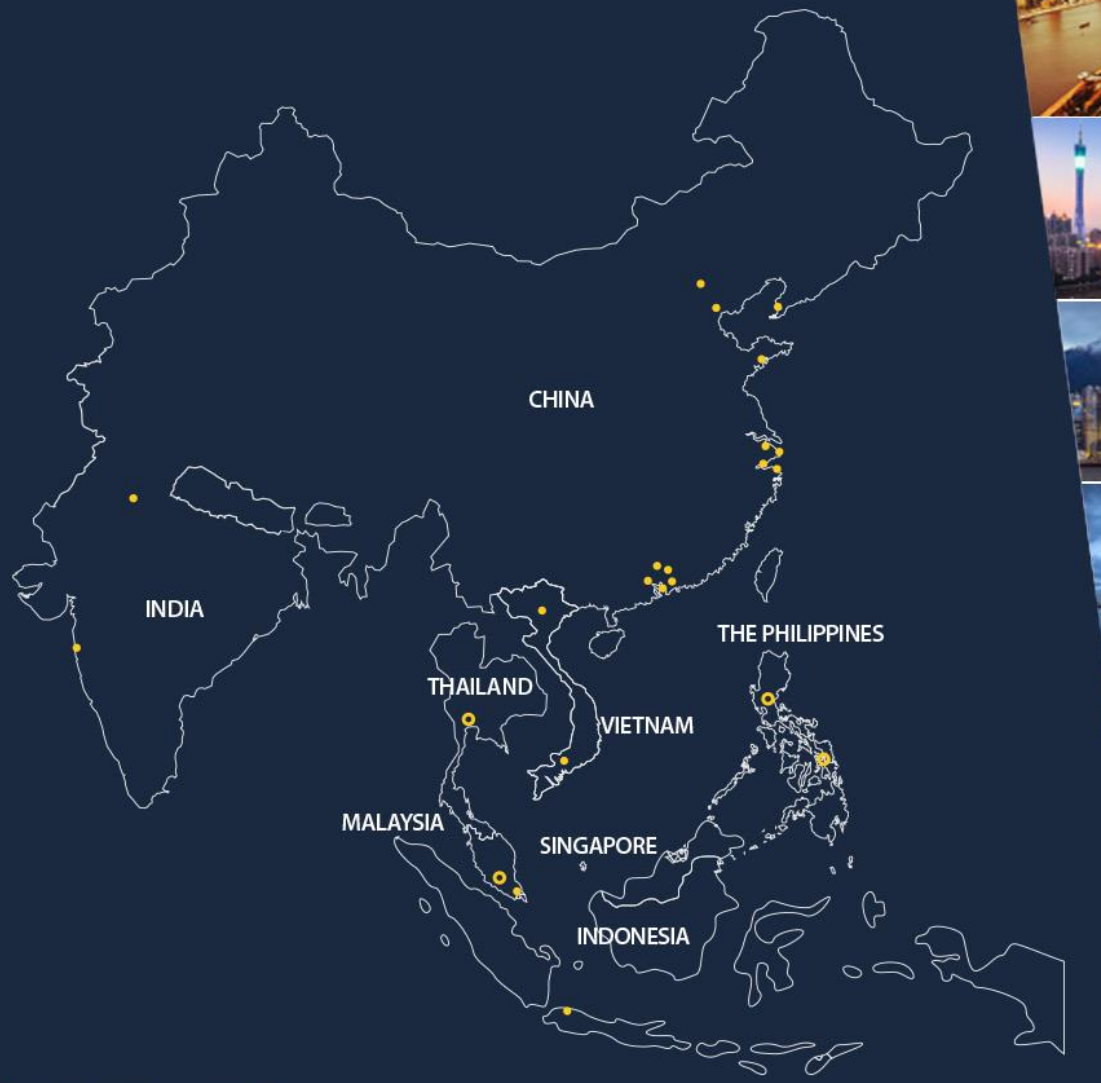
thomas.zhang@dezshira.com

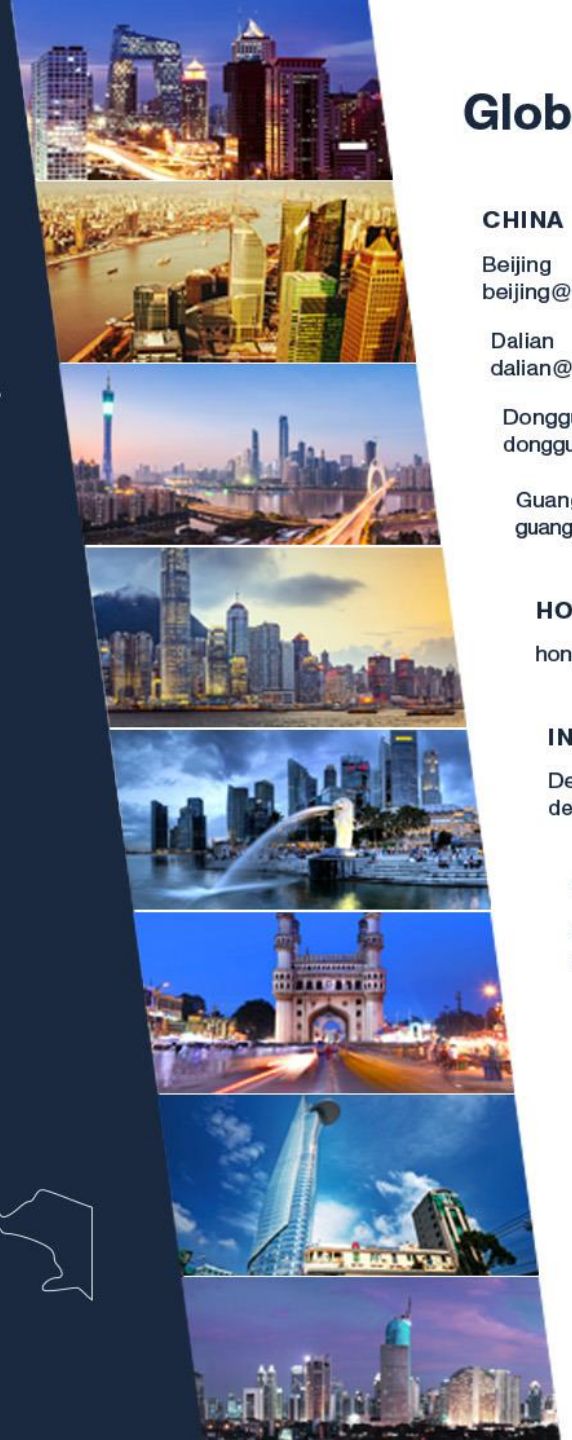
Follow Us

Scan the QR code for daily China updates including articles, events, new publications, and more

DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia





Global Offices

CHINA

Beijing
beijing@dezshira.com

Hangzhou
hangzhou@dezshira.com

Shenzhen
shenzhen@dezshira.com

Dalian
dalian@dezshira.com

Ningbo
ningbo@dezshira.com

Suzhou
suzhou@dezshira.com

Dongguan
dongguan@dezshira.com

Qingdao
qingdao@dezshira.com

Tianjin
tianjin@dezshira.com

Guangzhou
guangzhou@dezshira.com

Shanghai
shanghai@dezshira.com

Zhongshan
zhongshan@dezshira.com

HONG KONG

hongkong@dezshira.com

INDONESIA

indonesia@dezshira.com

SINGAPORE

singapore@dezshira.com

INDIA

Delhi
delhi@dezshira.com

Mumbai
mumbai@dezshira.com

VIETNAM

Hanoi
hanoi@dezshira.com

Ho Chi Minh City
hcmc@dezshira.com

DEZAN SHIRA ASIAN ALLIANCE MEMBERS

Malaysia
malaysia@dezshira.com

The Philippines
philippines@dezshira.com

Thailand
thailand@dezshira.com

DEZAN SHIRA LIAISON OFFICES

Germany
germandesk@dezshira.com

Italy
italiandesk@dezshira.com

United States
usa@dezshira.com

For more information, please visit **www.dezshira.com**

DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Scan this QR code

Visit our mobile page and
get the latest updates investors
news and resources with us