



DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia



CELEBRATING

China Cyber and Data Security Compliance

What Your Business Needs to Do

July 2022





DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia



- *Dezan Shira & Associates Offices*
- *Dezan Shira Asian Alliance Members*

Global Offices

CHINA

Beijing
beijing@dezshira.com

Guangzhou
guangzhou@dezshira.com

Qingdao
qingdao@dezshira.com

Suzhou
suzhou@dezshira.com

Dalian
dalian@dezshira.com

Hangzhou
hangzhou@dezshira.com

Shanghai
shanghai@dezshira.com

Tianjin
tianjin@dezshira.com

Dongguan
dongguan@dezshira.com

Ningbo
ningbo@dezshira.com

Shenzhen
shenzhen@dezshira.com

Zhongshan
zhongshan@dezshira.com

VIETNAM

Hanoi
hanoi@dezshira.com

Ho Chi Minh City
hcmc@dezshira.com

Danang
danang@dezshira.com

INDIA

Delhi
delhi@dezshira.com

INDONESIA
Jakarta
indonesia@dezshira.com

SINGAPORE
singapore@dezshira.com

Mumbai
mumbai@dezshira.com

Batam
batam@dezshira.com

HONG KONG
hongkong@dezshira.com

MONGOLIA
mongolia@dezshira.com

DEZAN SHIRA ASIAN ALLIANCE MEMBERS

Malaysia
malaysia@dezshira.com

The Philippines
philippines@dezshira.com

Thailand
thailand@dezshira.com

Bangladesh
bangladesh@dezshira.com

Cambodia
cambodia@dezshira.com

Japan
japan@dezshira.com

South Korea
southkorea@dezshira.com

DEZAN SHIRA LIAISON OFFICES

Germany
germandesk@dezshira.com

Italy
italiandesk@dezshira.com

United States
usa@dezshira.com

Please email asia@dezshira.com or visit www.dezshira.com



Resources for Asia Investors



www.asiabriefing.com

Asia Briefing, a subsidiary of Dezan Shira & Associates, publishes business magazines and guides for China, India, Vietnam, Singapore and other key nations in emerging Asia.



www.dezshira.com/library

Asiapedia is a collection of these resources based on the experiences we made on the ground.



All publications are available at DSA's online bookstore at www.asiabriefing.com/store

Today's Speaker



Kyle Freeman

Partner, International Business Advisory

Dezan Shira & Associates



Beijing, China



kyle.freeman@dezshira.com



Table of Contents

1. Regulatory Environment

- Key Regulations
- Enforcement Trends

2. Implications for Companies

- Data Classification
- Multi-Level Protection Scheme (MLPS)
- Cross-Border Data Transfer (CBDT)



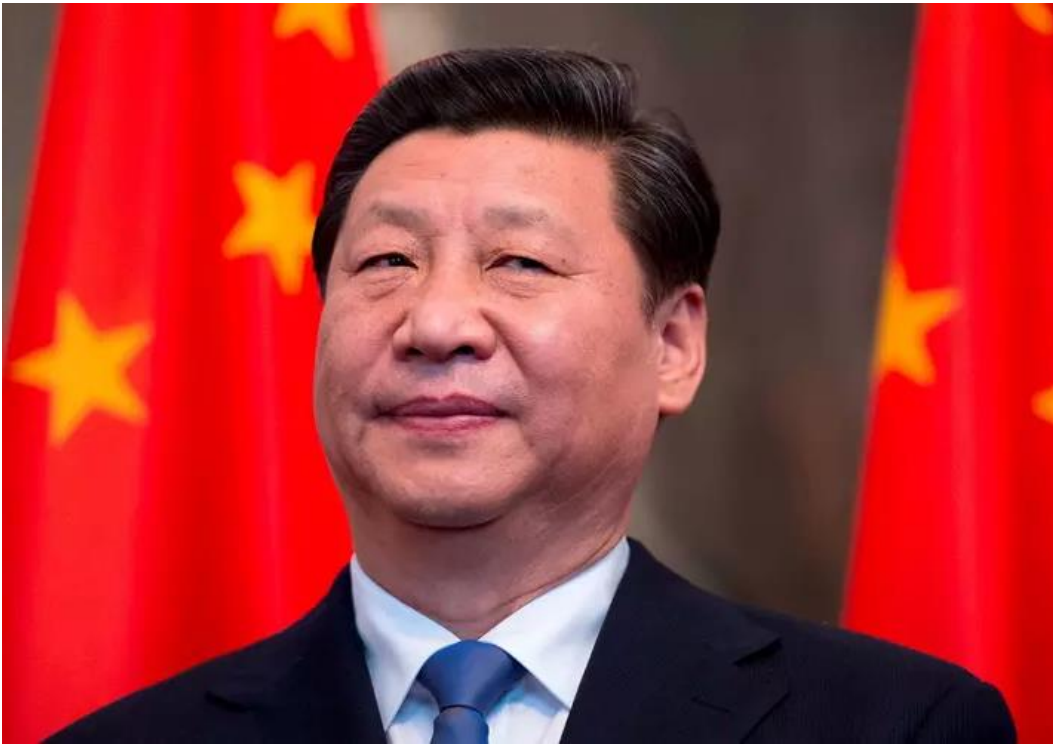
DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Regulatory Environment



CELEBRATING



“There is no national security without cybersecurity.

“The digital economy is related to the overall situation of national development, and data has become a key strategic resource that affects global competition in the digital economy era”

- Xi Jinping
President

“The importance of data come from its impact on national security. It does not necessarily depend on industries, but the nature and function of the data concerned.”

- Zuo Xiaodong
President of China Research Institute of Information Security

Key Cybersecurity & Data Regulations *timeline*



Cybersecurity Law (CSL)

effective
June 1, 2017



Data Security Law (DSL)

effective
September 1, 2021



Personal Information Protection Law (PIPL)

effective
November 1, 2021

Key Cybersecurity & Data Regulations *overview*

	Cybersecurity Law	Data Security Law	Personal Information Protection Law
Basics	<ul style="list-style-type: none"> ➤ 1st legislation devoted to supervision and management of cybersecurity and internet space in China 	<ul style="list-style-type: none"> ➤ Concerned primarily w/ data protection and data activities of entities 	<ul style="list-style-type: none"> ➤ Concerned primarily with personal and consumer information protection
Importance	<ul style="list-style-type: none"> ➤ Introduces key cybersecurity concepts (e.g. MLPS 2.0, critical information infrastructure operators (CIIOs)) ➤ Lays foundation for future laws 	<ul style="list-style-type: none"> ➤ Demonstrates “important” and “core” data significance for data protection ➤ Equates data security w/ national security; extraterritorial implications 	<ul style="list-style-type: none"> ➤ Sets fundamental requirements for handling of PI and sensitive PI for entities ➤ Regulates cross-border data transfer
Business Implications	<ul style="list-style-type: none"> ➤ <u>Overall</u>: Unique cybersecurity regime w/ increased authority oversight ➤ <u>Management</u>: Cybersecurity protection responsibility shifted from IT to management ➤ <u>Risk & Compliance</u>: Risk assessment and evaluation procedures for entities introduced ➤ <u>Operations</u>: CAC has increased power to use CSL for non-cybersecurity related issues 	<ul style="list-style-type: none"> ➤ <u>Overall</u>: Data security and data transfer strategies ➤ <u>Management</u>: Foreign business HQs must follow DSL while treating Chinese data abroad ➤ <u>Risk & Compliance</u>: “Important data” processors face extra requirements, incl. for cross-border transfer ➤ <u>Operations</u>: Data security review regime can open foreign business data activity to regulatory scrutiny 	<ul style="list-style-type: none"> ➤ <u>Overall</u>: Granular personal information protection requirements along data value chain ➤ <u>Management</u>: Foreign HQs must follow PIPL while treating Chinese citizen data abroad ➤ <u>Risk & Compliance</u>: Businesses must conduct impact assessment for cross-border PI transfer ➤ <u>Operations</u>: Enforcement activities for PIPL standards already underway



Key Cybersecurity & Data Regulations *content*



Cybersecurity Law (CSL)

- Multi-Level Protection Scheme (“MLPS”)
- Network Critical Device and Dedicated Products Testing and Certification
- Critical Information Infrastructure (“CII”) Security Protection
- Cybersecurity Review
- Cybersecurity Monitoring, Early Warning and Information Notification



Data Security Law (DSL)

- Data Classification and Grading Mechanism
- Important Data
- National Core Data
- National Security Review Mechanism
- Export Control
- Countermeasures
- Data Cross-Border Transfer
- Data Security Protection Obligations
- Data Transaction and License Requirement



Personal Information Protection Law (PIPL)

- Determination of Personal Information (“PI”)
- Basic Principles on PI processing
- Legal Basis
- Third-party Management
- Rights of PI Subjects
- Rules on Data Localization and Cross-Border Transfer
- PI Processor Obligations

Cybersecurity Law

	Cyber Security Review Measures		Data Security Law	
MLPS and Security Protection System Guidelines		Encryption Law	Personal Information Protection Law	
			Data Management Guideline	

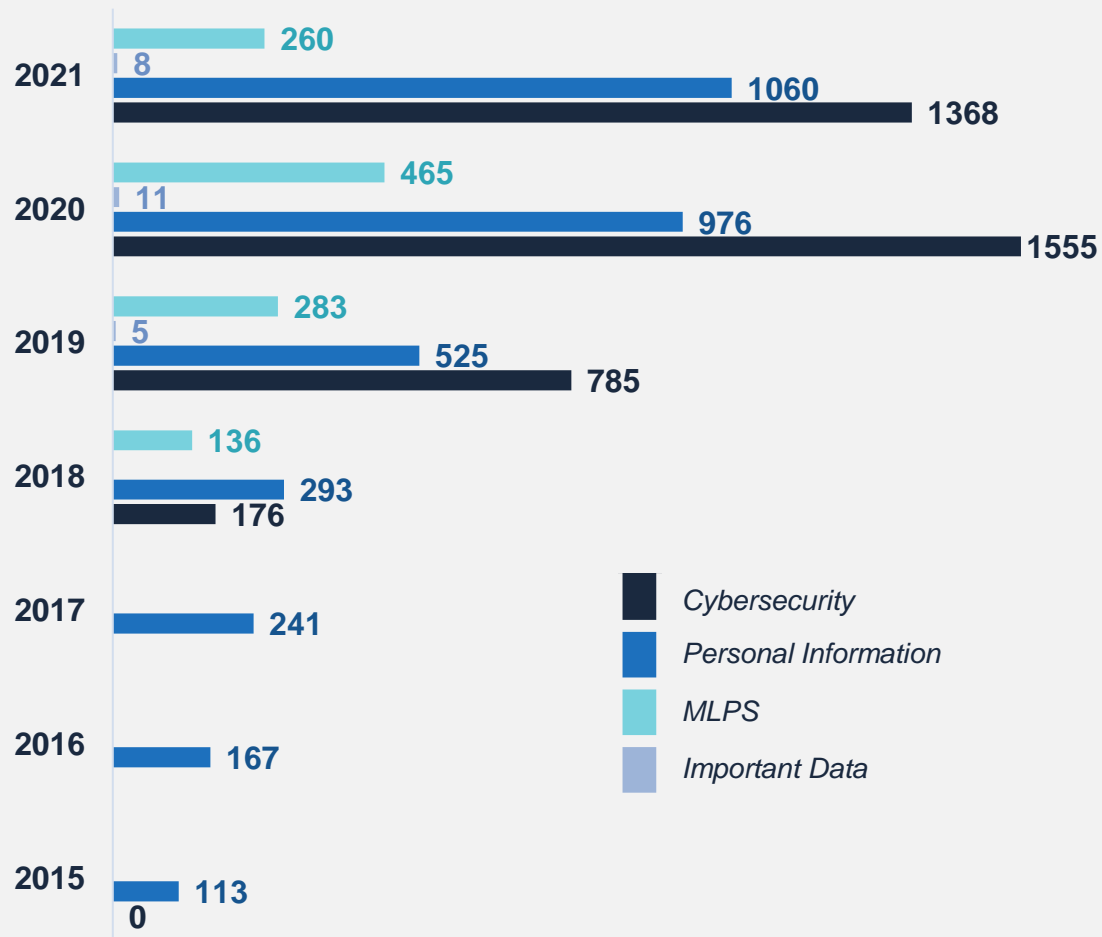
Grading Guidelines for Classified Protection	Security Protection of CII Regulations	Encryption & Algorithms	Consumer Rights Protection Law	Cross-Border Data Transfer Security Assessment Measures
MLPS Classification Guidelines	Basic Requirements for CII Network Security Protection	Commercial Encryption Management Regulations	Criminal Law (revised)	Security Assessment of Cross-Border Transfer of Personal Information and Key Data Measures
Baseline for MLPS Cybersecurity	CII Security Control Measures	Algorithm Recommendation Management Regulations	Civil Code (revised)	Measures to Promote Shanghai's Urban Digital Transformation (LP)
Implementation Guide for MLPS for Information Systems	<i>more regulations & standards expected</i>	Strengthening Comprehensive Management of Internet Information Service Algorithms Guiding Opinions	PI Security Specification	Beijing Plan for Creating Benchmark City for Global Digital Economy (LP)
Testing and Evaluation Guide for MLPS		Certification Rules for Commercial Cryptographic Products	Online PI Security Protection Guidelines	Important Data
General Requirements for MLPS of Cybersecurity I-IV		Opinions for Commercial Encryption Testing and Certification	PI Anonymization Guidelines	Important Data Identification Guidelines
Technical Requirements for MLPS Security Management Center		Testing and Evaluation For Information System Encryption Application	PI Security Impact Assessment Guidelines	MIIT Important Data Measures
Capability Requirements for Organization of MLPS		Network Protection	PI Security in Mobile Apps Guidelines	Automotive Important Data Measures
Technical Requirements for MLPS Security Design		Management of Network Product Security Vulnerabilities Regulations	Information Security Technology PI Notification Consent Guide	Data Classification Guidelines
		Network Key Equipment Security General and Technical Regulations	PI Security Engineering Guidelines	<i>more regulations & standards expected</i>
		General Requirements for Information System Encryption Application	Provisions on Scope Necessary PI for Common Types of Mobile Apps	
	Critical Information Equipment and Network Security Product Catalogue	Graduation and Evaluation for Effect PI De-Identification		
	Security Requirements for Database Management Systems	Interim Provisions on Mobile Internet App PIP management		
	General Requirements for Critical Network Equipment Security	Mobile Internet App PI Security Evaluation Specification		

New policy since 2021

Draft regulations

Enforcement













Administrative Penalties Issues (citing policies)



Enforcement Trends

- Areas of Focus
 - Enforcement of the Cybersecurity Law took off around 2019
 - Personal information protection rules, have been enforced even before the PIPL came into effect
 - Public Security Bureaus (PSB) have already started to reach out to companies to check MLPS compliance
 - Important data is not yet in the center of the enforcement yet
 - Ministry of Industry and Information Technology (MIIT) increasingly focused on handling of personal information in apps
- Foreign vs Domestic Companies
 - Majority of enforcement targets have been Chinese companies, but both local and foreign companies have been targeted for enforcement
- Companies also starting to use data protection rules in lawsuits

Enforcement *priorities & trends*

 Data Security	<ul style="list-style-type: none">➤ Data must be segmented and categorized according to regulations➤ Increased regulatory requirements for important and core data (e.g. localization)	 Enforcement Stage
 Personal Information Protection	<ul style="list-style-type: none">➤ New rules for consent notification and substantial fines➤ Increased enforcement actions for apps	 Enforcement Stage
 Cross-Border Data Transfer	<ul style="list-style-type: none">➤ General data processors may have to go through self-assessments when transferring data abroad➤ Security assessments by the CAC may be required for important data holders	 Advanced Draft Stage
 MLPS 2.0	<ul style="list-style-type: none">➤ Any network storing important data, in theory, is graded Level 3➤ Local PSBs reach out for compliance with MLPS 2.0 (with local characteristics)➤ Public-facing networks (e.g. websites) currently face more enforcement scrutiny	 Enforcement Stage
 Network Products	<ul style="list-style-type: none">➤ Network products now have more scrutiny through cybersecurity reviews➤ Network products can be part of important data➤ Vulnerability patching a critical aspect of data security value chain	 Enforcement Stage
 CIIOs & Encryption	<ul style="list-style-type: none">➤ Industry regulators define CIIOs in their sectors➤ Security review of network products for CIIOs➤ Certified encryption required for networks graded MLPS Level 2 or above	 Advanced Draft Stage

Critical Information Infrastructure Operators (CIIO)



**Public Communication &
Information Services**



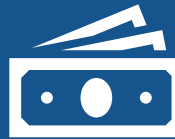
Energy



Water



Transport



Finance



Public Services



E-Government Services



National Defense



other important network facilities or information systems that may seriously harm national security, the national economy and people's livelihoods, or public interest in the event of incapacitation, damage, or data leaks.



DEZAN SHIRA & ASSOCIATES
Your Partner for Growth in Asia

Implications for Companies



Implication for Companies *simplified overview*



Transfer of HR / Customer Data	Transfer of “important” Business Data	Foreign Encryption	Software
Requires risk assessment and possibly approval	May require risk assessment and possibly approval	Might face difficulties to get license and could be opened to authorities	Might face difficulties to get license and could be opened to authorities
Information Networks in China	Critical Information Infrastructure	Network Products	
Are subject to a security grading and need to fulfill requirements based on their level	Machinery engineering unlikely to be affected itself, but customers may have demanding requirements	Network product providers and network operators must ensure they fulfill vulnerability security requirements	

data border

Extraterritorial Jurisdiction

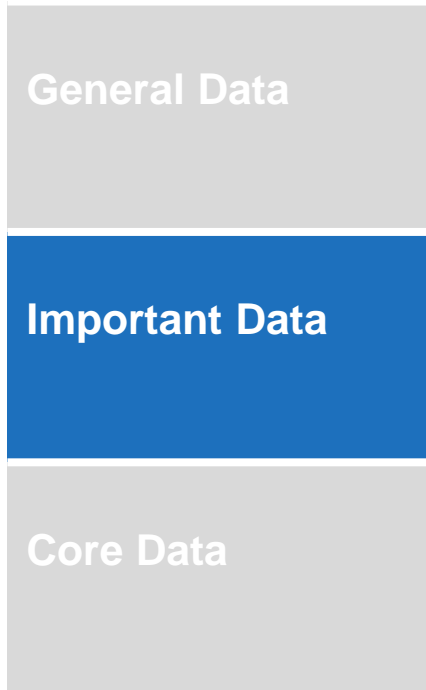
Foreign data need to sign contracts and ensure data protection on grounds of Data Security Law and Personal Information Protection Law

Data Classification *types*

	General Criteria	Industry Specific Criteria
General Data	Information that has a relatively low impact on the legal interests of individuals and organizations	Small impact on industry and infotech. (i.e. small number. of affected companies, low recuperation costs after misuse)
Important Data	Electronic data which, if altered, destroyed, disclosed or illegally obtained, may endanger national security and public interests	Large impact on functions and/or economic interests of industry and infotech., or causing serious production accidents
Core Data	Information that has great impact on China's data security in space, polar regions, the deep sea, and AI	Very serious impact, causing large-scale paralysis of networks or damage to production across industries

NOTE. MIIT framework categorized the industrial and IT data that could be classified as "important data", including R&D, production, operational, and platform data in industries such as raw materials, equipment, consumer goods, electronics, software and IT services. Some industry frame further outline specific data with specific classifications and requirements

Data Classification *important data*



Examples of Important Data

- Data on Operation of Economy – data on strategic reserves like grain, data on CIIO production process, etc.
- Data on Population & Health – data on healthcare, food & drug, etc.
- Data on Natural Resources & Environment – geographic data, map data, etc.
- Data on Science & Technology – export controlled items, important IP, inventions, etc.
- Data on Security Protection
- Data related to Service Providing
- Data related to Government Affairs

Important Data *compliance requirements*

	Legal Requirements	General Data	Important Data
Organizational	<ul style="list-style-type: none"> ➤ Identify person and body responsible for data security ➤ Set up and improve process of data security emergency / management system ➤ Set up internal catalogues of “important data”, including type, quantity and processing activities ➤ Organize data security education and training 	<ul style="list-style-type: none"> ✓ ✓ ✓ 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓
Compliance Procedures	<ul style="list-style-type: none"> ➤ File “important data” information w/ MIIT (industrial and IT data) ➤ Adhere to MLPS Level 3 and CIIO requirements for processing important data ➤ Cooperate w/ and assist domestic regulators in obtaining data ➤ File advance report on data access from overseas regulators ➤ Report to authorities w/in 8 hours of any “important data” security incidents ➤ Report progress to authorities w/in 5 workdays after incident ➤ Conduct risk assessments before cross-border data transfer 	<ul style="list-style-type: none"> ✓ ✓ 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓ ✓ ✓ ✓
Technical Requirements	<ul style="list-style-type: none"> ➤ Use backups, access control to prevent data security incidents ➤ Use encryption methods to protect important and core data 	<ul style="list-style-type: none"> ✓ 	<ul style="list-style-type: none"> ✓ ✓

Multi-Level Protection Scheme (MLPS) *classification*

	Level 1	Level 2	Level 3	Level 4	Level 5
Legal Persons	Damage	Serious Damage	Very Serious Damage		
Public Security		Damage	Serious Damage	Very Serious Damage	
National Security			Damage	Serious Damage	Very Serious Damage

NOTE: A network's protection level is graded according to its degree of societal impact within two benchmarks.

- 1. Importance of network w/ regards to national security, economic construction, and social life*
- 2. Level of harm network disruption or a cybersecurity incident could cause to national security, public order and interest, and the interest and lawful rights of related citizens, legal persons, and other organizations*

Multi-Level Protection Scheme (MLPS) *security review application procedures (1 of 2)*

1.	Initial Classification	<ul style="list-style-type: none">➤ Conduct a self-assessment and propose a defined protection level for their network according to the <i>Guideline for MLPS Classification</i>
2.	Registration w/ Local Police Agency	<ul style="list-style-type: none">➤ Systems or applications should be registered for MLPS within 30 days protection level is determined➤ Local police will review registration and may either approve registration and officially issue an MLPS Registration Certificate or reject application and require rectifications

Documents Required for MLPS Application

Required for Level 2 & Above

- *Multi-Level Protection Classification Report*
- *Multi-Level Protection Registration Application Form*
- *Expert Classification Review Opinion*
- *Network and Information Security Commitment*
- *MLPS Emergency Contact Registration Form*

Additional Requirements for Level 3 & Above

- *System Architecture and Topology Description*
- *Cyber Security Organization and Management Policy*
- *System Security and Protection Measures*
- *Security Product Inventory and Sale Permit*
- *System Classification Assessment Report*
- *Regulatory Agency Review and Approval*

Multi-Level Protection Scheme (MLPS) *security review application procedures (2 of 2)*

3.	Additional Security Review <i>(for Level 2 and above)</i>	<ul style="list-style-type: none">➤ Level 2 or above must engage a qualified expert to carry out additional security reviews➤ Qualified experts typically 3rd party agency but can be certified security professionals w/in company.➤ Review process similar to other security audits and technical assessments, qualified expert will:<ul style="list-style-type: none">▪ Interview IT management and technical staff; as well as security professionals, to understand current security governance and practices. They will also▪ Examine documented security design and related policies and procedures to assess whether appropriate security controls are within the requirements of said level➤ Minimum score of 75 is necessary to pass assessment for MLPS 2.0
4.	Assessment Verification by Approved Experts	<ul style="list-style-type: none">➤ Review evaluated and endorsed by independent expert recognized by MLPS regulatory body➤ Expert is required to provide official documents to confirm assessment results
5.	Government Approval	<ul style="list-style-type: none">➤ Assessment result and verification should be provided as supplementary documents to the branch of local police agency where the registration was filed➤ Documents are confirmed by Ministry of Public Security and official MLPS certification is issued
6.	Re-evaluation	<ul style="list-style-type: none">➤ Higher protection level, the more frequently re-assessments should be conducted:<ul style="list-style-type: none">▪ Level 2 networks re-assessed every 2 years▪ Level 3 networks re-assessed every year▪ Level 4 networks re-assessed every 6 months▪ Level 5 networks, re-evaluation defined and managed by regulatory ministry and commissions

Personal Information Protection Law (PIPL) *key features*

Individual Consent for Data Handling	<ul style="list-style-type: none">➤ Consent must be obtained prior any PI processing➤ All matters related to PI processing activities , including the identity and contact details of data recipients must be provided to data subjects
Organizational Governance	<ul style="list-style-type: none">➤ PI processors should appoint responsible person(s) for supervising the data activities on PI and security measures adopted for protecting PI➤ PI processors should adopt security measures to protect the PI collected (e.g. applying data encryption, providing security training and education to employees)
Rights of Individuals	<ul style="list-style-type: none">➤ Individuals can decide whether organizations can process their PI and to what extent, or to make changes, or delete the PI collected, and companies must establish appropriate mechanisms for data subjects to do so
Cross-Border Data Transfer (CBDT)	<ul style="list-style-type: none">➤ Cross-border PI transfer to only take place when “necessary”➤ Notify individual on CBDT arrangement, ways to exercise their rights, and obtain consent➤ CIIOs and PI Processors who meet data volume threshold (to be determined) set by CAC shall pass security assessment before cross-border data transfer can take place
Data Localization	<ul style="list-style-type: none">➤ CIIOs and PI processors who meet data volume threshold* set by CAC shall store all PI collected and generated within Mainland China
Extraterritoriality	<ul style="list-style-type: none">➤ PI protection requirements are extraterritorial: includes all PI gathered within PRC➤ Foreign firms require a PI representative in China

GDPR vs PIPL *key differences*



Scope



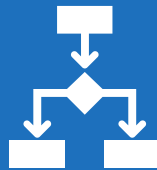
Definition of PI



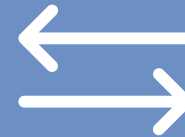
Definition of Roles



Processing PI Legal Basis



DPIA & PIPIA



Cross-Border Data Transfer



Compliance & Enforcement

	Similarities	Differences
Scope	<ul style="list-style-type: none"> ➤ Both are extraterritorial in application 	<ul style="list-style-type: none"> ➤ GDPR focuses more on where business is established ➤ PIPL focuses more on where PI processing activity happens
Definition of PI	<ul style="list-style-type: none"> ➤ Both have a similar definition for general PI, either direct or indirect ➤ Both subject some categories of PI to more stringent protection requirements (e.g. “special category” data in GDPR and “sensitive” PI in PIPL) ➤ Both define similar rights for individuals 	<ul style="list-style-type: none"> ➤ PIPL excludes anonymous information from the definition of PI ➤ PIPL has a much wider scope of what is considered “sensitive” PI than GDPR’s “special category” data
Definition of Roles	<ul style="list-style-type: none"> ➤ Both define different roles to distinguish between different positions in PI processing activities 	<ul style="list-style-type: none"> ➤ GDPR defines roles of data controller and data processor – PIPL defines role of PI handler (which is the same as the data controller) but not a data processor (or “entrusted party”) ➤ GDPR defines data protection officer (DPO) role, who is not liable for performance of their duties – PIPL defines role as “the person in charge of PI protection”, who is liable for performance of their duties; PIPL also defines the role of “representative”, which is a person appointed to communicate with Chinese authorities if the company doesn’t have physical presence in China but provides services or products to people in China. ➤ PIPL defines a “gatekeeper” role for large platforms

	Similarities	Differences
Legal Basis for Processing PI	<ul style="list-style-type: none"> ➤ Both define obtaining consent, performing contracts, legal obligations, vital interests, and public interest as the legal bases for processing PI 	<ul style="list-style-type: none"> ➤ PIPL requires “separate consent” in specific situations, such as processing sensitive PI or cross-border data transfer (CBDT) activities ➤ PIPL doesn’t define “legitimate interest perused by data controller” as a legal basis for processing PI ➤ PIPL explicitly allows processing of PI for news reporting
DPIA & PIPIA	<ul style="list-style-type: none"> ➤ Both require companies to assess potential risks to individual or data subjects before they can process their PI in certain circumstances 	<ul style="list-style-type: none"> ➤ PIPL calls it a Personal Information Protection Impact Assessment (PIPIA), while GDPR calls it Data Protection Impact Assessment (DPIA) ➤ GDPR defines scenarios in which a DPIA must be conducted rather ambiguously, requiring it when processing PI with new technology, creating a high risk for data subject ➤ The PIPL defines the scenarios in which a PIPIA must be conducted more specifically

	Similarities	Differences
Cross-Border Data Transfer (CBDT)	<ul style="list-style-type: none"> ➤ Both request recipient party to provide adequate protection for PI they receive and that level of protection should be equivalent to requirements of GDPR or PIPL 	<ul style="list-style-type: none"> ➤ GDPR defines a few channels for cross-border data transfer (CBDT), which include “adequacy decision” (for destination country), SCC, and BCR (for MNCs) ➤ GDPR allows CBDT when obtaining explicit consent from the data subject, for public interest, or for purposes of performing a contract ➤ PIPL CBDT rules are binding w/ other laws, such as CSL and the DS ➤ PIPL requests CBDT on the basis of “security assessment”, “certification”, or “standard contract with the recipient”
Compliance & Enforcement	<ul style="list-style-type: none"> ➤ Both define a supervisory authority that is responsible for regulating data (or PI) processing activities and enforcing protection rules 	<ul style="list-style-type: none"> ➤ Under GDPR, there is usually a single and independent supervisory authority with a clearly defined regulatory scope and supervisory procedures. ➤ Multiple supervisory authorities exist in China with interrelated responsibilities. This complicates communication and follow-ups during compliance processes.

DPIA & PIPIA *process*



Consultation w/ internal and external stakeholders throughout the process

Establish objectives and actions	Type of data	Apply data protection principles	Accept	Document status of each risk	Acceptance of final report
Appoint project team and management	Use of data	Assess individual risk	Reduce	Identify who will sign off	Review
Screening questions	Record in flowchart	Assess compliance risk	Eliminate	Prepare final report	Evaluate
Early Consultation	Record in information asset register	Assess other, related risks	Reject	Publish / deliver final report	Update

Cross-Border Data Transfer *example scenarios*

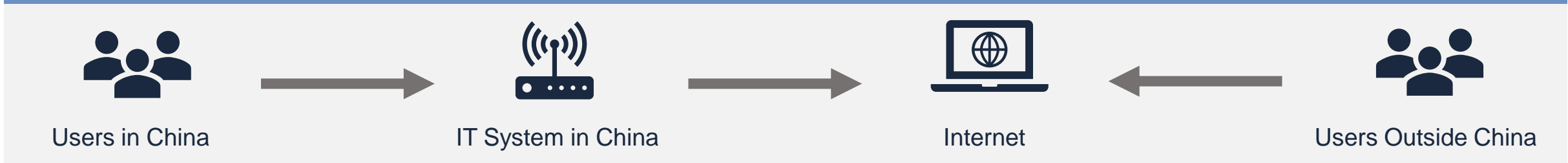
IT Systems Located in HQ Outside of China



IT System in China with Data Sync / Transfer with HQ



IT System in China That Allows Non-China Users to Access It



Cross-Border Data Transfer (CBDT) *Cyberspace Administration of China (CAC) security review thresholds*

Activities Requiring CAC Security Review

- Data processors providing “important” data overseas
- CIIOs and data processors that process PI of more than 1 million people providing PI overseas
- Data processors that have transferred the PI of over 100,000 people or the “sensitive” PI of over 10,000 people overseas since January 1 of the previous year
- Other situations required to declare data export security assessment as stipulated by the CAC

Sensitive PI



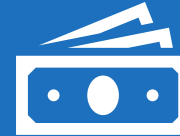
Biometric Data



Data on Religious Beliefs or Specific Identities



Medical History



Financial Accounts



Location & Whereabouts



PI of Minors Under 14

Cross-Border Data Transfer (CBDT) *CAC security review process*

1.	Conduct Self Assessment	Company	
2.	Submit Application to CAC	Company	
3.	CAC Accepts Application	Government	w/in 7 working days <i>of application</i>
4.	CAC Security Assessment	Government	w/in 45 working days <i>of acceptance notice</i>
5.	Objections to Assessment Results & Request for Re-Assessment <i>(if applicable)</i>	Company	w/in 15 working days <i>of receiving results</i>
6.	Reapply for Authorization <i>(if company intends to continue processing or transferring data overseas after expiration of authorization)</i>	Company	60 working days before <i>before expiration</i>

Documents to be Submitted to CAC for Security Review:

1. A declaration
2. Cross-border data transfer risk self-evaluation report
3. Legal documents to be signed between data processor and overseas recipient
4. Other materials required for security assessment work



Self Assessment Criteria

- Legality, legitimacy, and necessity of purpose, scope, and method of the CBDT, and the processing of data by overseas recipient
- Scale, scope, type, and sensitivity of data being transferred, and possible risks that CBDT could pose to China's national security, public interests, and legal rights of individuals and organizations
- Responsibilities and obligations undertaken by overseas recipient and whether management and technical measures and capabilities for fulfilling responsibilities and obligations can ensure security of outbound data
- Risk of the data being tampered w/, destroyed, leaked, lost, transferred, or illegally obtained or used during overseas transfer or after it exits country, and whether channels for safeguarding rights and interests of PI are unobstructed
- Whether data export-related contracts or other legally binding documents ("legal documents") that are entered into w/ overseas recipient fully stipulate responsibility and obligations of data protection
- Other matters that may affect the security of data export

Legal Document Requirements

- Purpose and method for data transfer and scope of data being transferred; what overseas recipient needs data for and methods they will use to process it
- Where and for how long data will be stored overseas; processing measures for exported data after data storage time limit is up, stipulated objectives have been achieved, or legal documents have been terminated
- Binding requirements for the overseas recipient to transfer the data to another organization or individual
- Security measures that will be taken if there is a substantive change in overseas recipient's control or operating scope, or if there is a change to security protection policies and regulations of region where data is being transferred to, a change to network security environment, or other force majeure circumstances that make it difficult to guarantee security of data
- Remedial measures, liabilities for breach of contract, and dispute resolution methods for breaching data security protection obligations stipulated in legal documents
- Requirements for proper emergency response and channels and methods to protect individuals' rights to safeguard PI if outbound data is at risk of being tampered w/, destroyed, leaked, lost, transferred, or illegally obtained or used

Implications for Companies *example for standard business procedures*



Human Resources *(staff in China)*

- Design and implement data privacy policy
- Distribute and receive employee consent for:
 - Personal Information Processing Notification
 - Personal Information Processing Consent Letter (for Regular Personal Information)
 - Personal Information Processing (for Sensitive Personal Information)
- Add personal information protection chapter to Staff Handbook (and implement through democratic process)



Business Transaction

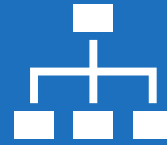
- Understand and segment / classify data collected during business transactions
- Conduct DPIA or PIPIA (if needed)
- Add or update existing business contracts to incorporate appropriate data and cybersecurity clauses
- Design and implement data protection; as well as other cybersecurity, measures to required compliance level

What Should Companies Do



Strategy

- Assess and monitor (future) risks for IT strategy and services
- Set 2022 objectives to ensure cybersecurity compliance
- Prioritize action items



Organization

- Assign clear responsibilities for cybersecurity
- Build coordination mechanisms
- Strengthen legal-IT coordination capacities



Compliance

- Ensure compliance w/ PI protection regulations
- Segment data
- Conduct MLPS 2.0 self-assessments
- Conduct cross-border data transfer (CBDT) self assessment
- Ensure compliance of network equipment



DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Kyle Freeman

Partner

International Business Advisory

kyle.freeman@dezshira.com



Scan this QR code

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