
Morgan Lewis
TECHNOLOGY MARATHON
China's Privacy Regime –
What tech companies need to know
Lesli Ligorner, Todd Liao, and Sylvia Hu
Thursday, June 30th
© 2022 Morgan, Lewis & Bockius LLP

Presenters

K Lesli Ligorner

Todd Liao

Sylvia Hu

Morgan Lewis

Overview of Legal Framework for Data Protection in China

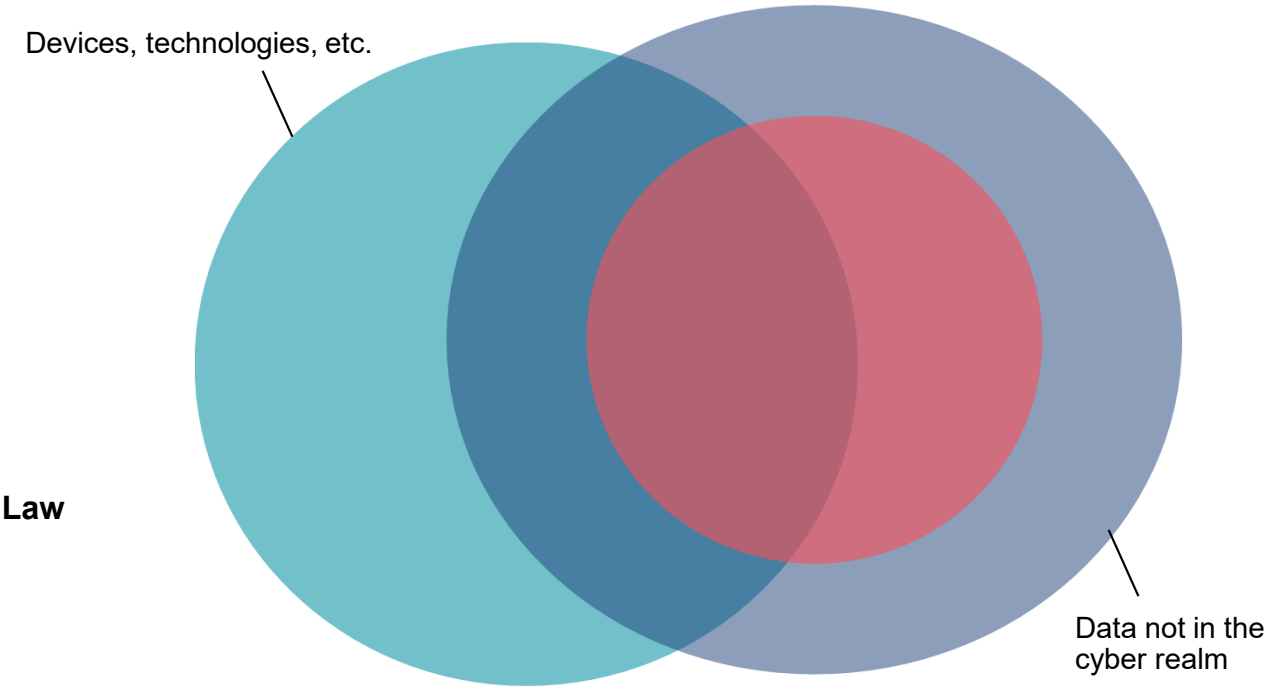
Morgan Lewis

Legal Framework for Data Protection in China

Cybersecurity Law

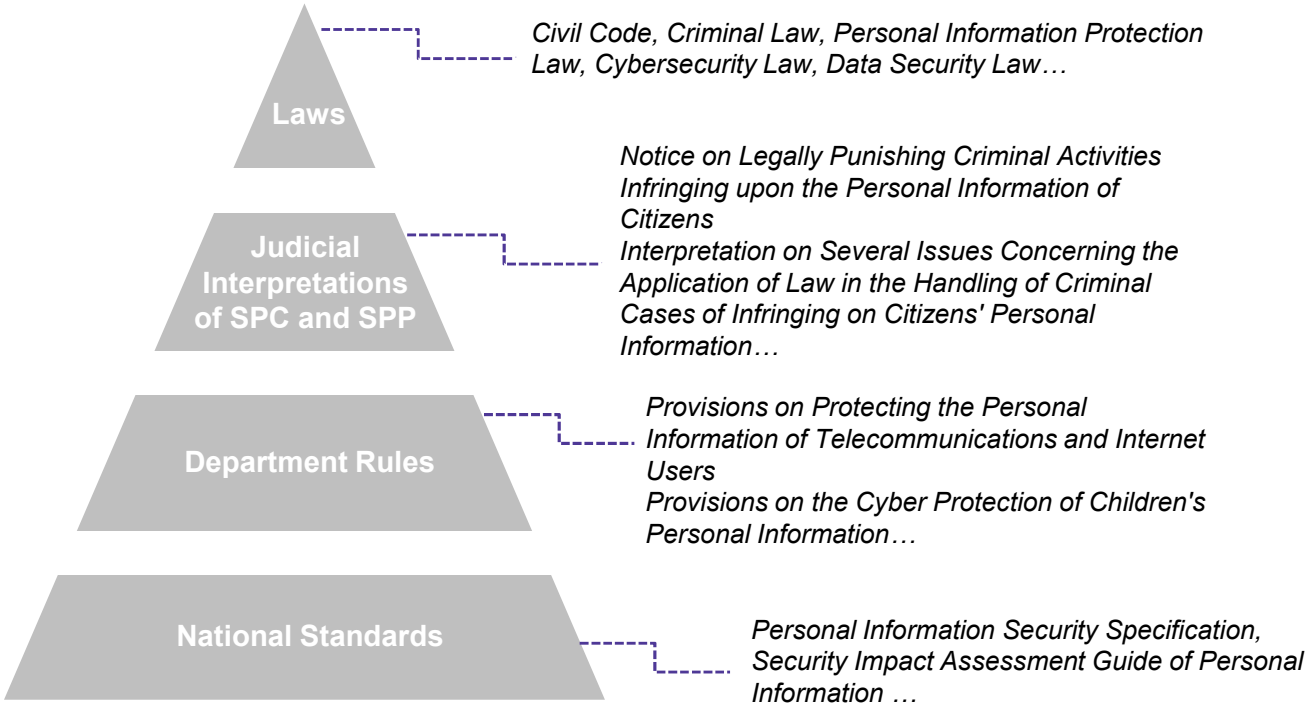
Data Security Law

Personal Information Protection Law



Legal Framework for Data Protection in China

LEGAL FRAMEWORK



Milestone Legislation

- **Cybersecurity Law ("CSL")**
- **Data Security Law ("DSL")**
- **Personal Information Protection Law ("PIPL")**

Foundations in the CSL in 2017, more details on data in PIPL and DSL.

Legislative Updates

- Cybersecurity Law (“CSL”)
  - Ties network operators to cybersecurity protection obligations
  - Introduces data localization
  - Imposes stricter obligations on critical information infrastructure operators
- Data Security Law (“DSL”)
  - Focuses on national security
  - Defines core data and important data
  - Outlines requirements for cross-border data transfers
- Personal Information Protection Law (“PIPL”)
  - Primarily about privacy of individuals
  - Defines personal information and sensitive personal information
  - Regulates their collection, processing, and transfer
  - Details on cross-border transfer of personal information

Legislative Updates – Data Security Law (Sept. 1, 2021)

Application scope and jurisdiction

Data

Art. 3 (1) **Data** refers to any information recorded in electronic or other form.

Data processing

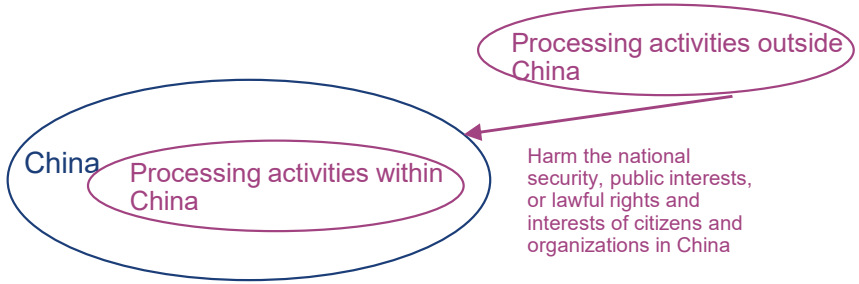
Art. 3 (2) **Data processing** includes collection, storage, use, processing, transmission, provision and disclosure of data.

Data security

Art. 3 (3) **Data security** refers to ensuring that data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security.

Territorial scope – Extraterritorial jurisdiction

Art. 2
(1) Data processing activities within China; and
(2) Data processing activities outside China that harm the national security, public interests, or lawful rights and interests of citizens and organizations in China



Legislative Updates – Data Security Law

Data categorization and protection

Data categorization

Art. 21 China will establish a "categorical and hierarchical system" based on the "importance of the data in economic and social development as well as the extent of harm to national security, public interests, or lawful rights and interests of individuals or organizations that would be caused once the data is tampered, destroyed, leaked, or illegally obtained or used."

Important Data
Data related to national security, economic development and social public interests.

→ **Conduct risk assessment** on a regular basis and submit the risk assessment report to the relevant competent authority

National Core Data
Data related to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests.

→ **Stricter management system**
A fine of up to RMB 10 million, cancellation of business licenses, and even criminal penalties

Legislative Updates – Data Security Law

Systems for data security reviews and export control

Data security reviews

Art. 24 The state is to establish a data security review system and conduct national security reviews for data processing activities that affect or may affect national security.

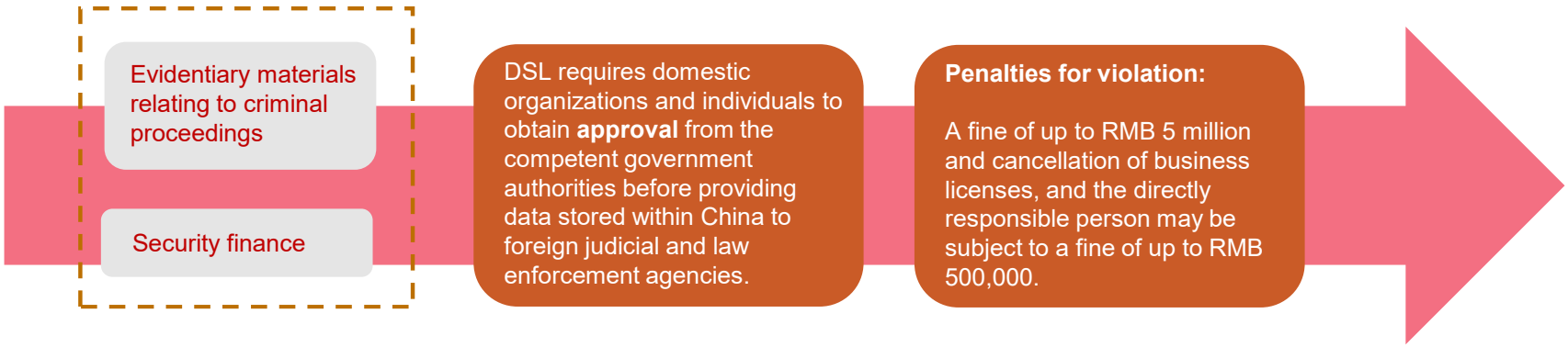
Security review decisions made according to law are final decisions.

Export control

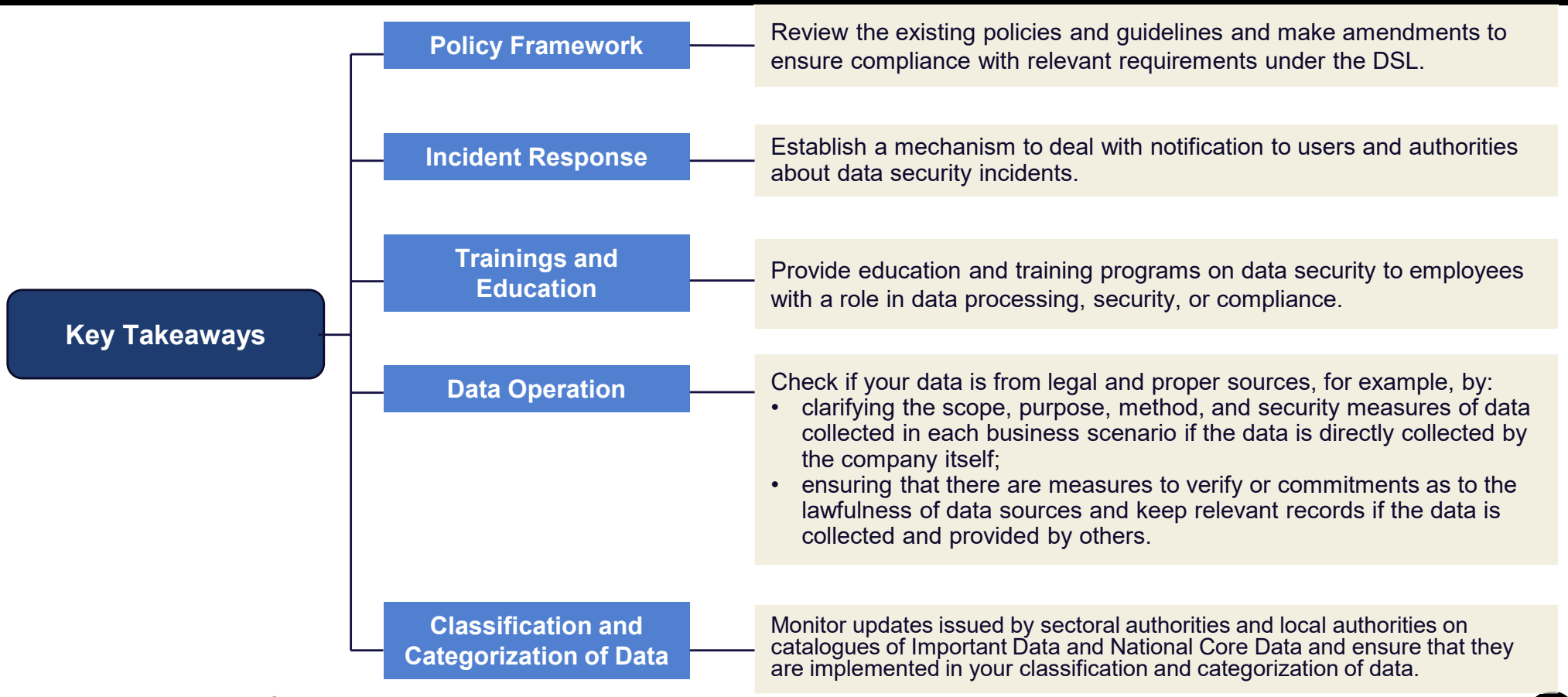
Art. 24 The state is to implement export controls in accordance with law for data belonging to controlled categories in order to safeguard national security and interests and fulfill international obligations.

Legislative Updates – Data Security Law

Restrictions on data transfer to foreign authorities



Legislative Updates – Data Security Law



Legislative Updates – Personal Information Protection Law

Definition of key terms

Personal information

Art. 4 **Personal information** is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization processing.

Sensitive personal information

Art. 28 **Sensitive personal information** means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons, grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

Legislative Updates – Personal Information Protection Law

Legal bases for processing

consent	Art. 13 (1) obtaining individuals' consent – separate consent required for certain situations, e.g. processing sensitive PI
contract **HR functions**	Art. 13 (2) necessary to conclude or fulfill a contract, or necessary to conduct human resources management;
legal obligation	Art. 13 (3) necessary to fulfill statutory duties and responsibilities or statutory obligations;
health and safety	Art. 13 (4) necessary to respond to a public health emergency, or in an emergency to protect the safety of individuals' health and property;
news/media reporting	Art. 13 (5) for purposes of carrying out news reporting and media monitoring for public interests;
disclosed already	Art. 13 (6) processing of personal information that is already disclosed;
miscellaneous	Art. 13 (7) other circumstances as required by laws.

Legislative Updates – Personal Information Protection Law

Personal information rights

- Right to information
- Right to access
- Right to correction/rectification
- Right to erasure/deletion
- Right to object to and restrict the processing of an individual's data
- Right to data portability (but needs to satisfy conditions stipulated by the Cyberspace Administration of China (CAC))
- Right to choose whether to be subject to automated decision-making
- Right to withdraw consent
- Right to raise a complaint with the regulator

Legislative Updates – Personal Information Protection Law

Legal liabilities and penalties

Administrative Penalties	Art. 66 of the PIPL a fine of not more than 50 million CNY, or 5% of annual revenue
Civil Liabilities	Art. 69 of the PIPL Where the processing of personal information infringes upon personal information rights and interests and results in harm, and personal information processors fail to prove they are not at fault, they shall take responsibility for the infringement through compensation, etc.
Criminal Liabilities	Art. 253 of the Criminal Law Infringement of Citizen's Personal Information
Public Interest Lawsuit	Art. 70 of the PIPL If the processing entities infringe the rights and interests of a large number of individuals, the People's Procuratorate and other designated organizations may file public interest lawsuits.

Hot Issues Affecting Tech Companies

Morgan Lewis

Hot Issues Affecting Tech Companies

- Data Localization and Cross-Border Transfer
  - Security assessment by the government authority
  - Certification by a qualified institution
  - Standard Contract
- Multi-Level Protection Scheme (MLPS)
- Specific Regulations on Mobile Applications (Apps)

Data Localization and Cross-Border Transfer

Cross-border Transfer of Personal Information

- Obtain separate consent of data subjects
- Carry out an internal risk assessment prior to cross-border transfer, and keep records of such transfers (Art. 55)
- Choose one of the following mechanisms to transfer personal information abroad (Art. 38)
  - ✓ undergo a security assessment administered by the CAC (for CII operators and entities that transfer important data and a large volume of personal information);
  - ✓ obtain certification from "qualified institutions" in accordance with the rules of the CAC;
  - ✓ enter into a transfer agreement with the overseas recipient based on a "standard contract" to be published by the CAC; or
  - ✓ other transfer mechanisms permitted under other laws and regulations.

Data Localization and Cross-Border Transfer - Security assessment

Critical information infrastructure operators (CIIO)	• Personal information and important data should be stored within China • Cross-border data transfers are subject to a government-led security assessment (and are not permitted if they bring risks to the national security, public interests, or data subjects' rights).
Non-CIIOs	The following data should be stored in China and subject to security assessment for cross-border transfer: • Personal information exceeding an amount threshold designated by CAC. • Important data.
Sector-specific regulation	Sector-specific regulations will also apply (Example: health big data and population health information).

Data Localization and Cross-Border Transfer - Security assessment

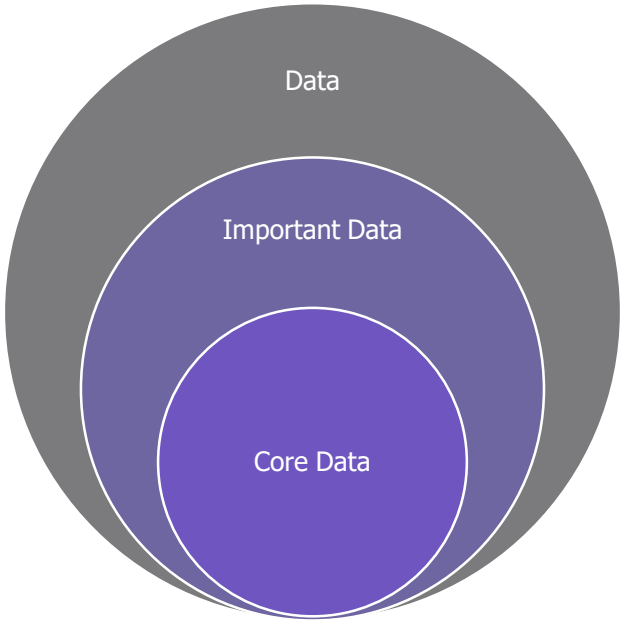
Triggering Criteria for Mandatory Government-led Security Assessment under the draft Security Assessment Measures

Key Factors	Triggering Criteria
Based on the "**special identity**" of the data controller	CIIO
	Operators who possess personal information of over a million users
Based on the "**sensitivity and scale**" of the data to be transferred abroad	The data to be transferred includes "important data"
	Cross-border transfer of personal information of over 100,000 individuals or sensitive personal information of over 10,000 individuals
Other factors	Other situations to be determined by the CAC

Regardless of whether the data transfer by a data processor triggers a CAC-led security assessment, the data processor is required to conduct a risk self-assessment on its data export before transferring any data outside of the PRC.

Important Data - Security assessment

The DSL did not provide a clear scope of "important data," but empowered regional and industry authorities to formulate specific catalogs.



Three Level of Data

Data that may fall under the scope of Important Data (Based on Important Data Categorization Guidelines)			
Oil & Gas	Coal	Petrochemistry	Electric Power
Communication	Electronic Information	Steel	Non-ferrous metals
Equipment Manufacturing	Chemical Industry	Defense Industry	Other Industries
Geographic Information	Civilian Nuclear Facility	Transportation	Postal Express
Water Resources	Population & Health	Finance	Credit
Food & Drug	Statistics	Meteorology	Radio & TV
Marine Environment	E-commerce	Others	

Data Localization and Cross-Border Transfer - Certification

On June 24, 2022, China published the final version of the Certification Specification for Cross-Border Processing of Personal Information.

1. Application scope: (i) among affiliates and subsidiaries; and (ii) by overseas data controllers.

2. To get a certification, the data exporter and recipient should satisfy the following requirements:

    - sign a data transfer agreement that contains required clauses;
    - appoint a data protection officer and set up a data protection department;
    - establish and comply with a uniform set of data processing rules;
    - conduct the personal information protection impact assessment before the cross-border data transfer;
    - take required measures to ensure the data subjects' rights are protected.

3. The list of qualified certification institutions has not been published.

Data Localization and Cross-Border Transfer - Standard Contract

On June 30, 2022, China published the draft version of the long-awaited standard contract for the cross-border transfer of personal information.

1. Applicable only if all the following are satisfied:

- Non-CIIO
- Operators who process personal information of no more than 1 million individuals;
- Since January 1 of the previous year, the cumulative amount of personal information provided overseas has not reached 100,000 individuals;
- Since January 1 of the previous year, the cumulative amount of sensitive personal information provided overseas has not reached 10,000 individuals.

2. Data exporter should conduct the personal information protection impact assessment (PIPIA);

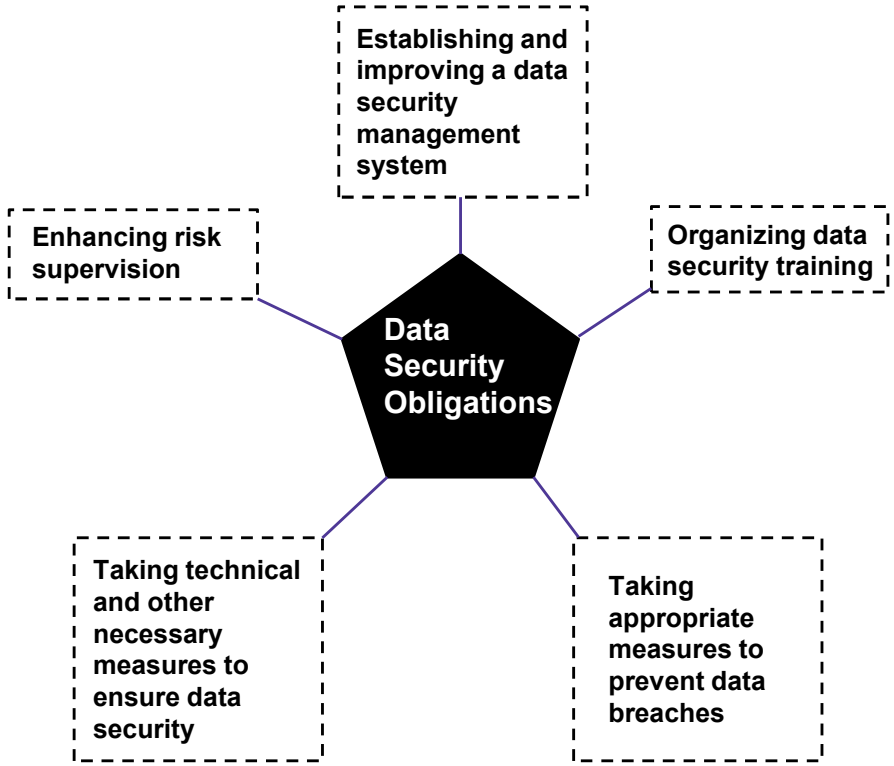
3. Data exporter should file the standard contract and the PIPIA report with the provincial competent government authority within 10 working days after the standard contract takes effect.

Multi-Level Protection Scheme (MLPS)

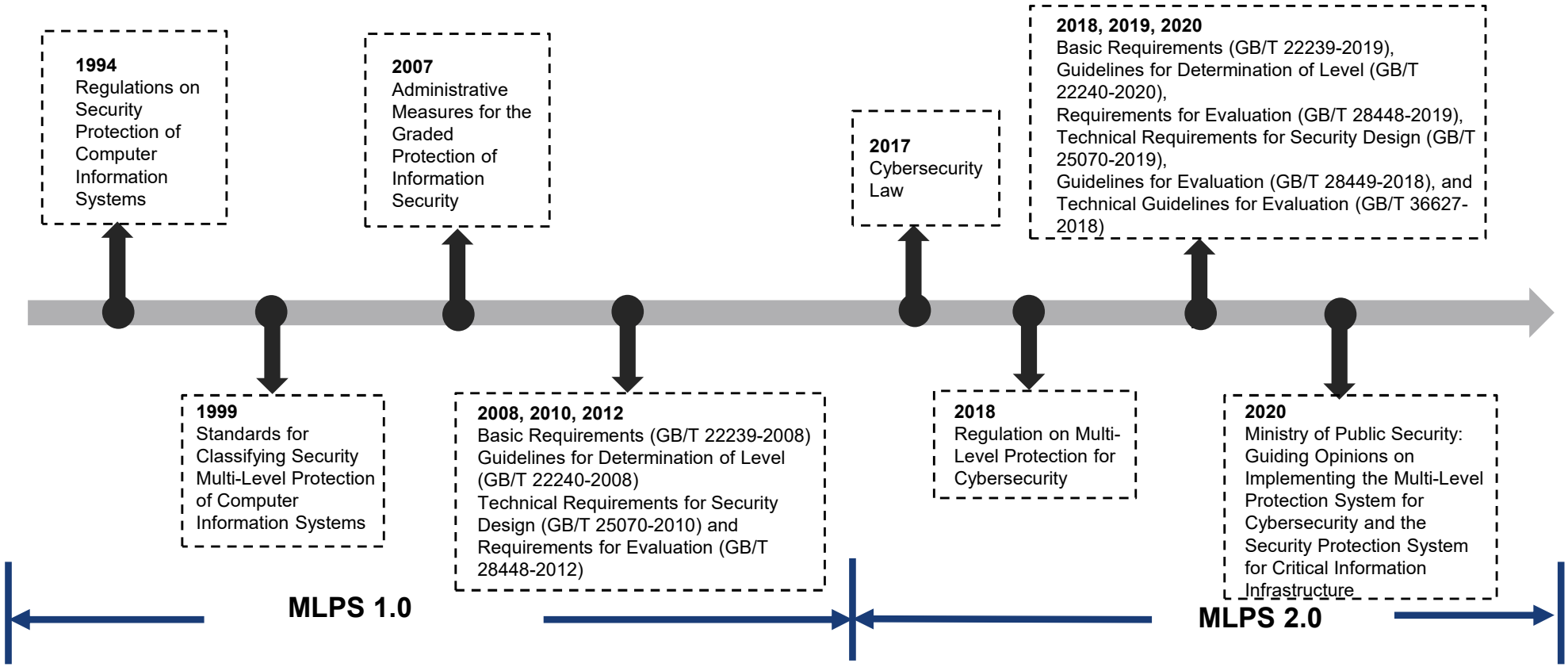
MLPS requirements and data security obligations

Multi-Level Protection Scheme

- Article 21 of the CSL provides that the country shall implement the rules for graded protection of cybersecurity.
- Article 27 of the DSL reemphasizes the importance of the MLPS by requiring all entities in China to carry out data processing activities in compliance with the data security requirements under the MLPS.



Multi-Level Protection Scheme



Multi-Level Protection Scheme

Definition

Multi-level protection scheme for cybersecurity refers to the multi-level protection and multi-level supervision and administration of networks (including information systems and data), the multi-level management of cybersecurity products, and the multi-level response to and disposal of security incidents occurring in the network.

Targets

The targets in the multi-level protection for cybersecurity are the systems that are composed of computers or other terminals and relevant equipment to collect, store, transmit, exchange and process information in accordance with certain rules and procedures, mainly including basic information networks, cloud computing platforms/systems and big data applications/platforms/funds, IoT, industry control system and systems employing mobile interconnection technology, etc. (Article 5.1 of Basic Requirements for Multi-Level Protection for Cybersecurity)

Procedures

Self-assessment

↓

Preliminary determination of Level

↓

Expert verification

↓

Filing with local PSB

↓

An official MLPS certification is issued

Multi-Level Protection Scheme

Determining the Steps for MLPS

Step 1

Prerequisite

- The system should be physically located in mainland China (including systems deployed on the cloud)

Type of server	Location
Application Server	Should be deployed in China
Database Server	Should be deployed in China

Step 2

Determine impact level of business information security

- Impact of data breach is based on the volume of personal information and sensitive personal information stored in the system
- Includes systems that cause social impact in case of problems, such as downtime or loss of sensitive information other than personal information

Level	Total amount of sensitive PII	Total amount of PII
Level 1	0-1,000	0-10,000
Level 2	1,000-10,000	10,000-100,000
Level 3	10,000-100,000	100,000-1,000,000
Level 4	≥100,000	≥1,000,000
Level 5		

Step 3

Determine impact level of system service security

- Impact of system failure to business operation is based on the importance of the system

Level	Importance of the system
Level 1	Low important system
Level 2	Medium important system
Level 3	High important system
Level 4	Extremely important system (only applicable to systems owned by State-owned enterprise or financial institution)
Level 5	

Multi-Level Protection Scheme

Proposed Compliance Path for MLPS 2.0

- Enterprises should identify systems and generate a system inventory based on the enterprises' operations and plans.
- Based on the identified grading objects and their levels, enterprises should perform gap analysis with reference to the MLPS requirements and produce self-assessment reports.
- Prepare grading documentation, arrange external expert reviews (level 2 or above), obtain approvals from authorities (where applicable), and submit filings to the relevant public security organs.
- Formulate security plans and determine cybersecurity tasks and their priorities, costs, and resources based on cybersecurity governance goals and findings from the MLPS assessment.

Specific Regulations on Mobile Applications (Apps)

Technology sector specific regulations follow the general principles under PIPL, DSL and CSL, but they impose additional privacy and cybersecurity obligations.

- *Method for Identifying the Illegal Collection and Use of Personal Information by Apps (2019)* ("**Method**") describes 31 specific types of illegal personal information activities and divides them into 6 categories.
  - "Failure to inform the data subjects of the data collection and use rules"
  - "Failure to expressly state the purpose, method and scope of collecting and using personal information"
  - "Collecting or using personal information without the consent of users"
  - "Collecting personal information unrelated to the services they provide in violation of the principle of necessity"
  - "Providing others with personal information without the consent"
  - "Failure to provide the function of deleting or correcting personal information in accordance with the law" or "failure to provide complaints channels"

Specific Regulations on Mobile Applications (Apps)

- ***Administrative Provisions on Mobile Internet Application Information Services (2022)*** **establish general requirements for App providers to :**
  - authenticate the real identity information of the users applying for registration. If users fail to provide real identity information, application providers shall not provide relevant services to them. (Art. 6)
  - deploy technical measures to ensure data security and establish a full-process data security management system (Art. 11)
  - not, for any reason, force users to consent to personal information processing, or refuse to provide their basic functions and services on the ground when users don't agree to provide unnecessary personal information. (Art. 12)
  - publish privacy notices (Art. 16.1)

Key Takeaways

Proactive steps to mitigate the compliance risks that MNCs may face:

- **Perform data mapping** to understand categories and location of data and identify important data, personal information, and sensitive personal information that the company is processing.
- **Perform a gap analysis** of the current data-related policies, both internal employee notice and external-facing privacy notices and policies, to comply with the informed consent requirements.
- **Establish a risk assessment process** for major data processing activities, covering the processing of important data, (sensitive) personal information, and cross-border data transfer, including the internal assessment and government reporting obligations.
- **Conduct the MLPS** as soon as possible.
- **Understand the localization requirements** and (if required) implement localized storage within China.
- **Understand the App-specific requirements** and take actions to be fully compliant.

K LESLI LIGORNER

K Lesli Ligorner
Shanghai / Beijing
+86.21.8022.8777
lesli.ligorner@morganlewis.com

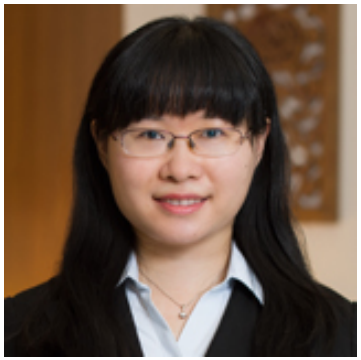
K Lesli Ligorner has more than 20 years of experience serving clients on a wide range of labor and employment matters, with nearly 15+ of those years spent on the ground in China. She has been advising a broad range of financial services; telecommunications, media, and technology; life sciences; and general manufacturing clients on the full suite of employment issues in China, including involving hiring and termination, and discrimination and harassment policies, training, and investigations. Lesli is admitted to practice in New York and New Jersey. Lesli's practice further includes compliance counseling and training covering establishment and enforcement of company policies, the Foreign Corrupt Practices Act (FCPA) and local anticorruption compliance, export controls, data protection and cybersecurity issues, and employment and anticorruption due diligence in mergers and acquisitions and related internal investigations.

TODD LIAO

Todd Liao
Shanghai/Boston
+86.21.8022.8799
todd.liao@morganlewis.com

Todd Liao works with clients on a wide range of financial transactions and legal issues involving China. He frequently works with multinational corporations on cross-border mergers and acquisitions, foreign direct investment and investment financing, disposal of Sino-foreign joint ventures and assets, and the structuring of complex commercial transactions. Todd also handles data privacy matters in China. Todd helps clients on developping proactive data breach contingency plans and assist in data breach prevention, including training, governance and risk assessments, data loss prevention strategies, and vendor management.

SYLVIA HU



Sylvia Hu
Shanghai
+86.21.8022.8527
sylvia.hu@morganlewis.com

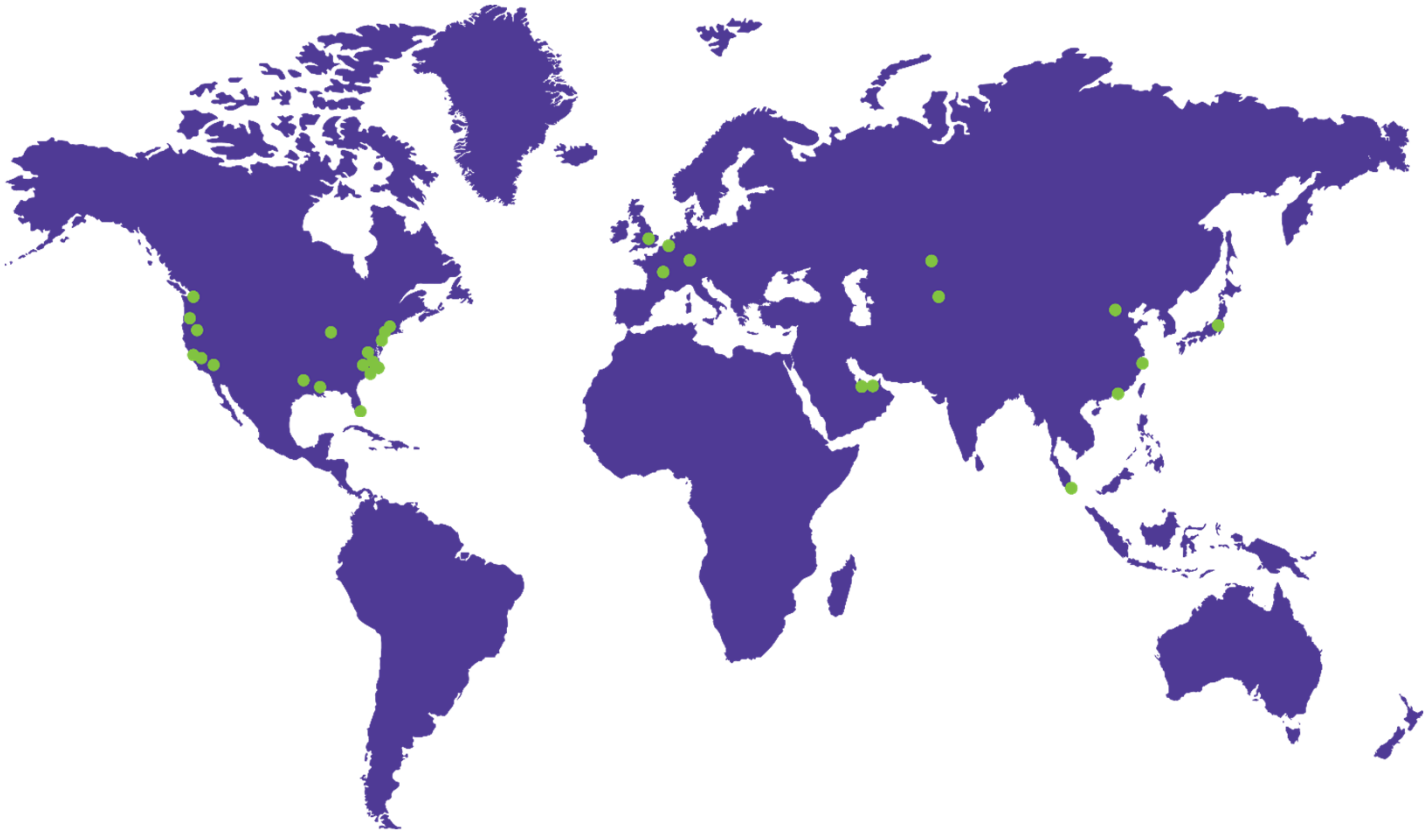
Sylvia Hu focuses on China's data protection laws, including those that involve data collection, privacy, storage, cross-border transfers, China's state secrets, and sector-specific areas such as life science and finance industries. She also advises multinational clients on foreign direct investment, Chinese employment law, and US Foreign Corrupt Practices Act (FCPA) practice in China.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU