
Morgan Lewis
THE NEW DATA PRIVACY AND CYBERSECURITY LAW IN CHINA
January 20, 2022
Todd Liao
© 2021 Morgan, Lewis & Bockius LLP

Morgan Lewis

Todd Liao

Contents

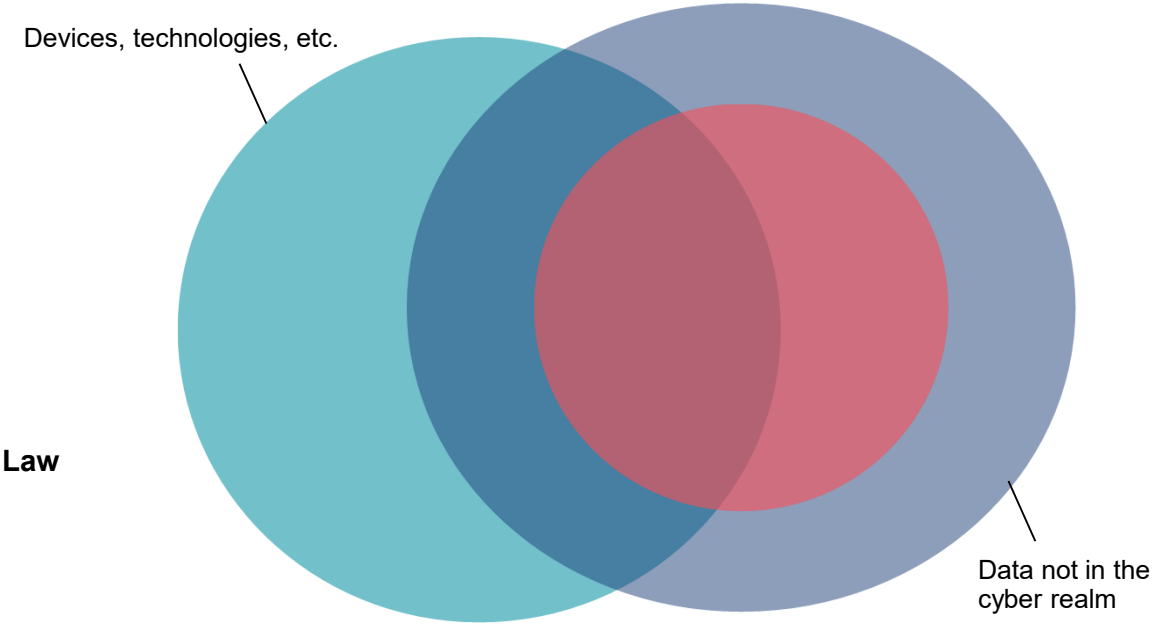
Legal Framework of Data Protection in China

VENN DIAGRAM

Cybersecurity Law

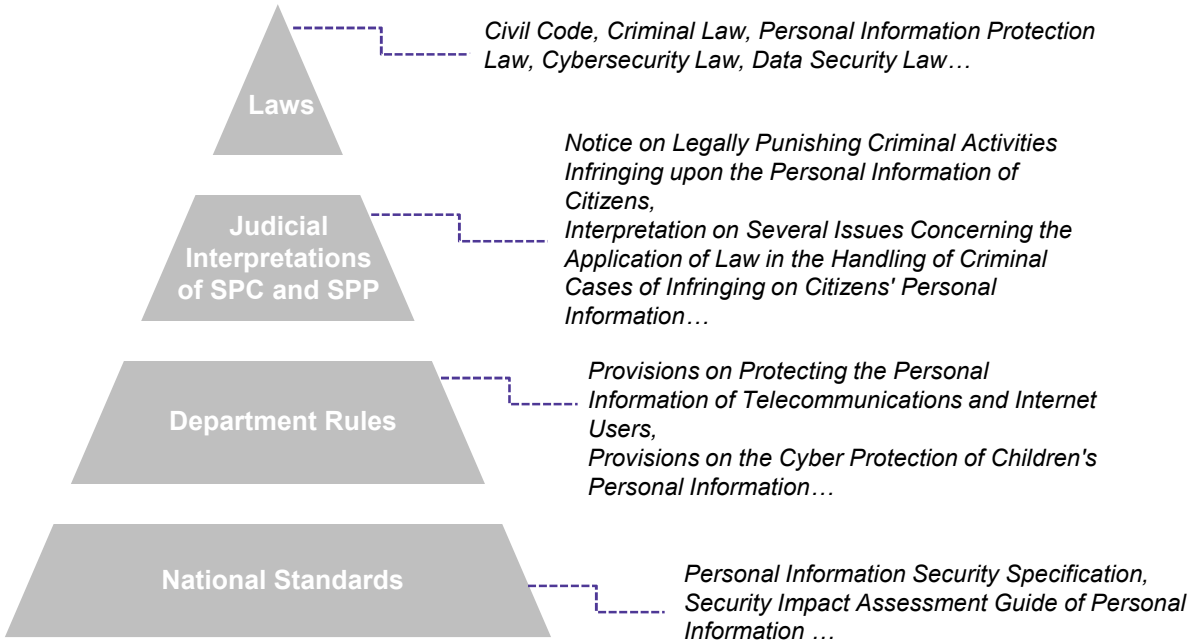
Data Security Law

Personal Information Protection Law



Legal Framework of Data Protection in China

LEGAL FRAMEWORK



Specific Rules in different sectors

- **Pharmaceutical Sector**

e.g., Measures for the Administration of Population Health Information

- **Financial Sector**

e.g., Implementation Measures for Protecting Financial Consumers' Rights and Interests

- **Automobile Sector**

e.g., Several Provisions on the Administration of Automobile Data Security (Trial)

.....

Legislative Updates

Two Milestone Legislation After the 2017 Cyber Security Law

- Data Security Law
- Personal Information Protection Law

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

Application scope and jurisdiction

Data

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

Data processing

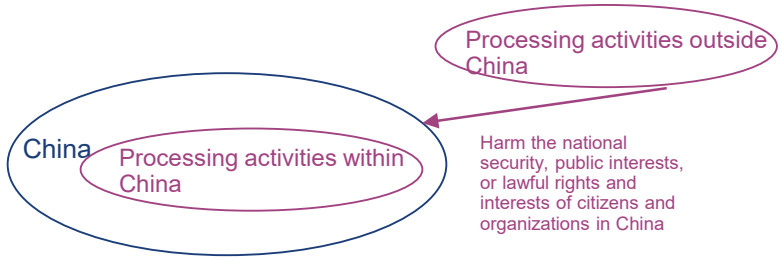
Art. 3 (2) **Data processing** includes collection, storage, use, processing, transmission, provision and disclosure of data.

Data security

Art. 3 (3) **Data security** refers to ensuring 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.
No concise scope of important data.

→ **Risk assessment**

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

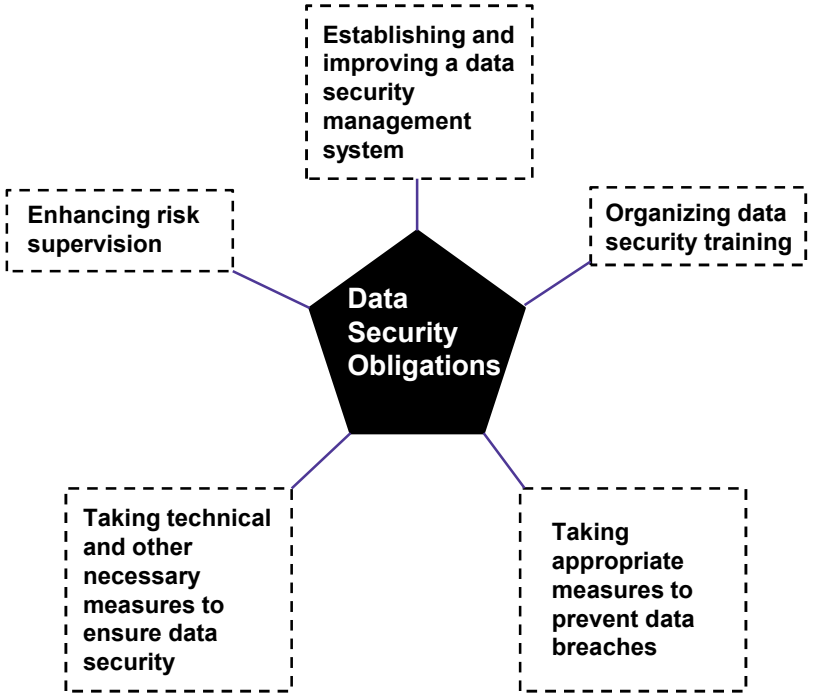
→ **Stricter management system**
A fine of up to RMB 10 million, cancellation of business licenses, and even criminal penalties

Legislative Updates – Data Security Law

MLPS requirements and data security obligations

Multi-Level Protection Scheme

- MLPS certification is a complex technology standard that requires companies to assess the current state of their information and network systems with servers located in China and the risks associated with them.
- Companies are required to evaluate and determine the level to which the company's information and network systems belong—from the lowest level 1 to the highest level 5.
- More administrative procedures (like filing with authority) are required if a company is classified as level 2 or above.



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.

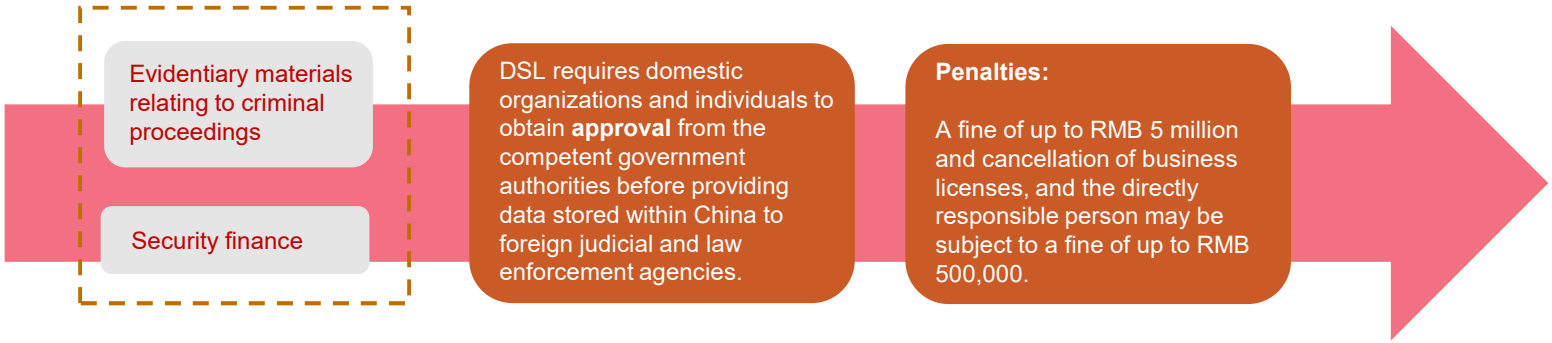
Security review decisions made according to law are final decisions.

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

Key takeaways

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	Art. 13 (2) necessary to conclude or fulfill a contract, or necessary to conduct human resources management;
obligation	Art. 13 (3) necessary to fulfill statutory duties and responsibilities or statutory obligations;
interest of natural person	Art. 13 (4) necessary to respond to a public health emergency, or in an emergency to protect the safety of individuals' health and property;
public interest	Art. 13 (5) for purposes of carrying out news reporting and media monitoring for public interests;
disclosed	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)
- Right to choose whether to be subject to automated decision-making
- Right to withdraw consent
- Right to bring a complaint with the regulator

Legislative Updates – Personal Information Protection Law

Cross-border Transfer of Personal Data

- Obtain separate consent
- Carry out an internal risk assessment prior to cross-border transfer, and keeping 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 (requirements for CII operators and processing entities that transfer a large volume of personal information);
  - ✓ obtain certification from "professional 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
  - ✓ transfer mechanisms in other laws and regulations (or the CAC presumably through implementing regulations).

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 Yuan, 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.

Legislative Updates – Personal Information Protection Law

Key takeaways

1

When collecting and using personal information:

- Post a well-designed privacy policy on website and/or deliver privacy notice to data subjects (customers and employees) that complies with statutory requirements
- Obtain separate consent from data subjects in certain scenarios

2

Before exporting personal information of Chinese individuals, take steps to fulfill the consent requirement and the data localization requirements:

- Provide required information to data subjects, including the method by which data subjects exercise the rights, and obtain separate consent from the data subjects.
- Know and comply with the data localization requirements.

Hot Issues/Top Requests From Clients

- Data Localization and Cross-Border Transfer
- Multi-Level Protection Scheme
- Personal Information Impact Assessment

Data Localization and Cross-Border Transfer Under the DSL, PIPL and Security Assessment Measures on Cross-Border Data Transfer

CIIOs

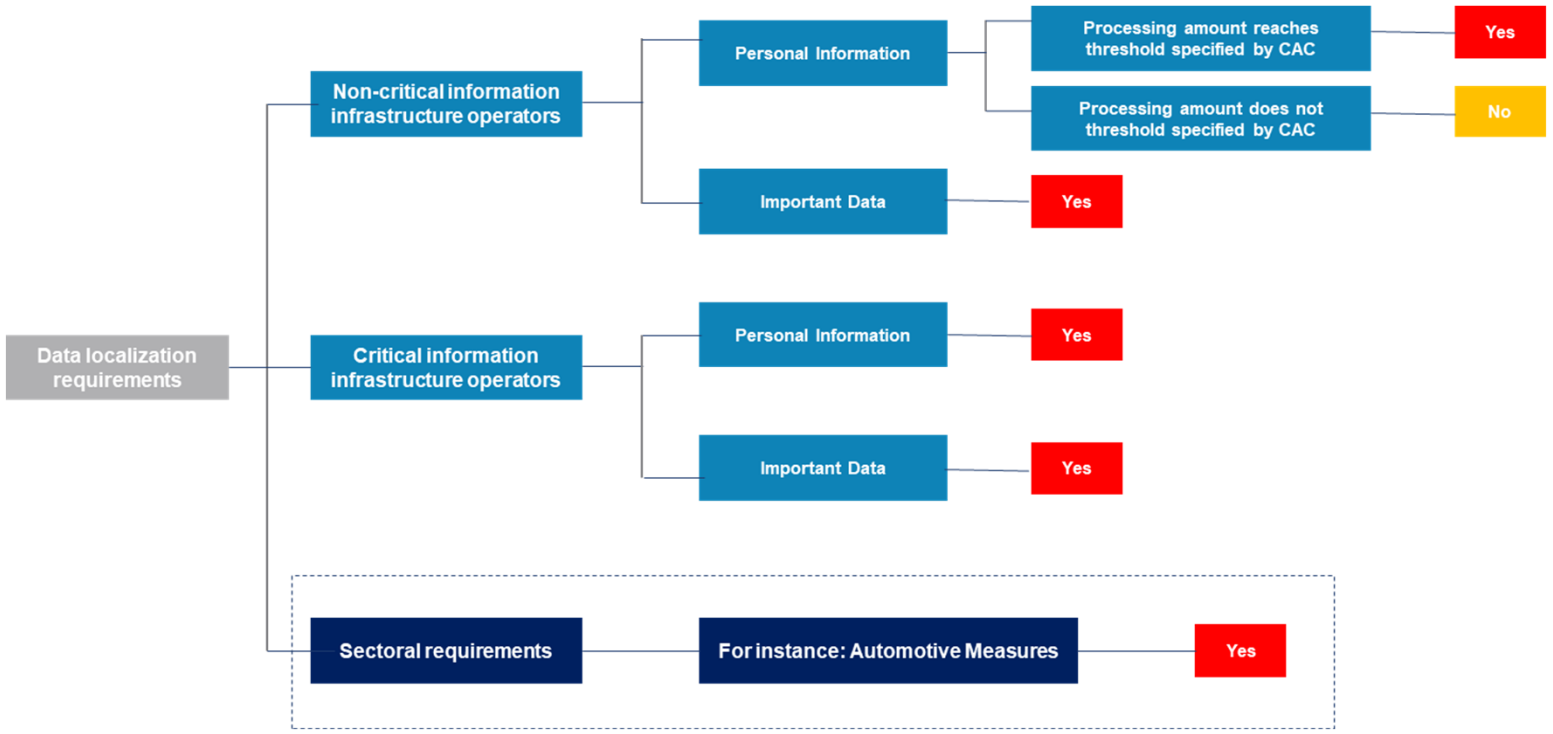
- Personal information and important data should be stored within China.
- Cross-border data transfers are subject to a government security assessment (and are not permitted if they bring risks to the national security, public interests, or data subjects' rights).

Non-CIIOs

- The following data should be stored in China and subject to security assessment for cross-border transfer:
  - Personal information and sensitive information exceeding an amount threshold designated by CAC.
  - Important data.

Companies in certain industries, sector-specific regulations will also apply (Example: health big data and population health information).

Data Localization and Cross-Border Transfer



Data Localization and Cross-Border Transfer

Triggering Criteria for Mandatory CAC-led Security Assessment Under the 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 "**sensitiveness 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

No matter whether the data transfer by a data processor triggers a CAC-led security assessment, the data processor is required to conduct risk self-assessment on its data export before transferring any data outside of the PRC.

Data Localization and Cross-Border Transfer

Seven Different Focus Areas of Assessment

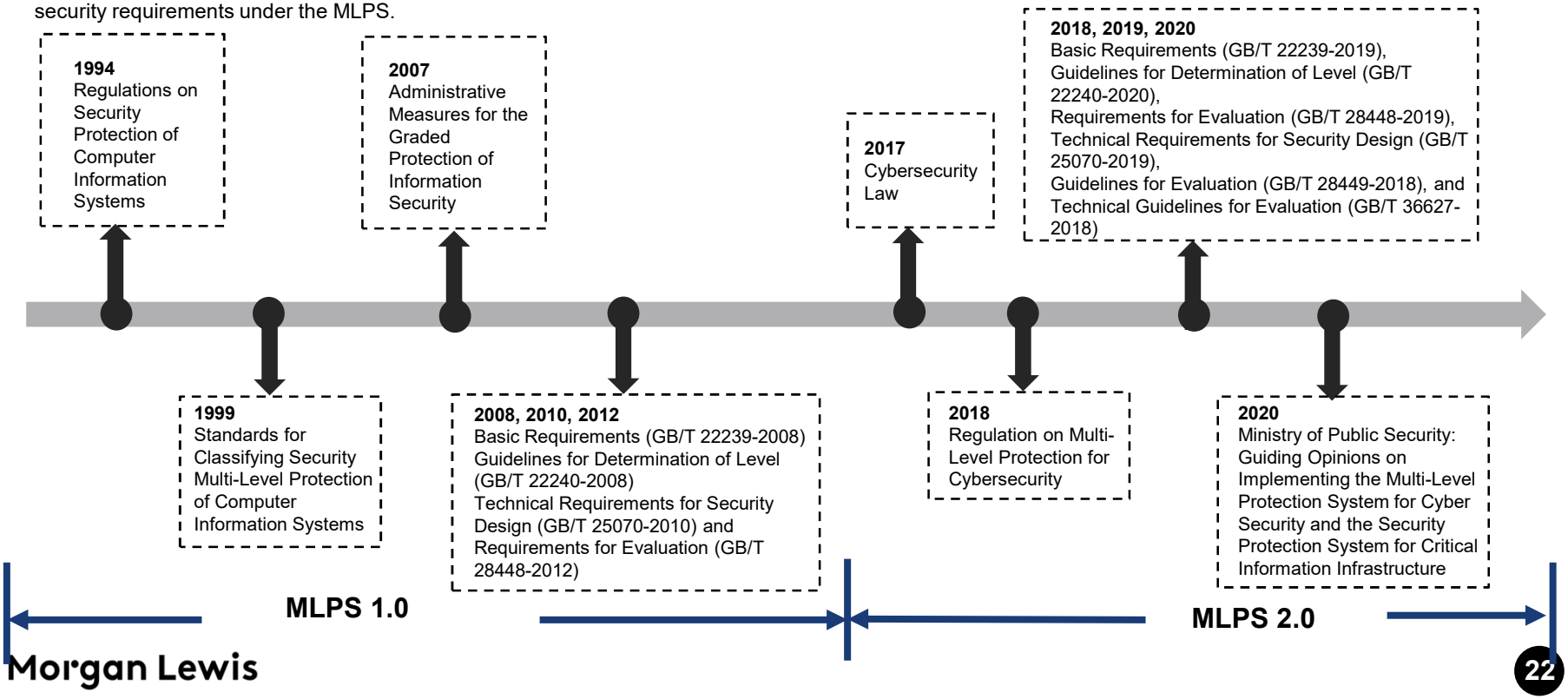
- Lawfulness, Justification, and Necessity
- Data Protection Level of the Overseas Recipient
- General Risk
- Protection of Data Security and Personal Information Rights
- Contracts Related to Data Export
- Compliance with Laws
- Other Matters

Application documents

- The application form, the risk self-assessment report on the data export, the contract or other legal binding document to be entered into by the data processor and the overseas recipient, and other documents and materials required for security assessment.

Multi-Level Protection Scheme

Article 21 of the CSL provides that the state 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

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

Determination Steps of 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 PII data and sensitive PII data 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.

Personal Information Impact Assessment

Under the PIPL, companies should conduct a PIIA before the following data processing activities:

- Processing sensitive personal information
- Using personal information to conduct automated decision-making
- Entrusting third parties to process personal information, providing personal information to third parties, or publishing personal information
- Providing personal information abroad
- Other personal information processing activities that will impose a major influence on individuals

Questions?

Morgan Lewis

Todd Liao

Partner
Morgan Lewis
todd.liao@morganlewis.com
+86.21.8022.8799

- Todd Liao works with clients on a wide range of privacy, financial transactions and legal issues involving China. Co-Head of Privacy and Cybersecurity Practice Group
  - 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. Variety of complex and novel cyber investigations and cases
  - Todd also handles intellectual property (IP) work, specifically assisting clients with managing their trademark portfolios.
  - Todd counsels on matters related to the US Foreign Corrupt Practices Act (FCPA) practice in China and throughout the Asia-Pacific region.
  - He advises multinational corporations regarding compliance with the FCPA and other regulatory compliance matters including policies and practices, gifts, travel and entertainment policies and violations, third-party due diligence issues, managing and conducting investigations of alleged FCPA violations, whistleblower investigations, and employee disciplinary actions.

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.

THANK YOU