Morgan Lewis

CHINA'S NEW PRIVACY LAW AND OTHER REGULATORY DEVELOPMENTS AFFECTING THE AUTOMOTIVE INDUSTRY

March 23, 2022

Todd Liao
Lesli Ligorner
Sylvia Hu

Morgan Lewis Automotive Hour Webinar Series

Series of automotive industry focused webinars led by members of the Morgan Lewis global automotive team. The 8-part 2022 program is designed to provide a comprehensive overview on a variety of topics related to clients in the automotive industry. Upcoming sessions:

MAY 18 | Part I: All Things Autonomous—Regulatory and Commercial Considerations for AVs

JUNE 15 | Automotive Finance and Consumer Protection Developments

JULY 13 | Part II: All Things Autonomous—Regulatory and Commercial Considerations for Delivery Robots (On and off campus), Escooters, and Drones

SEPTEMBER 14 | Part I: All Things EV—Regulatory and Commercial Considerations

SEPTEMBER 28 | Part II: All Things EV—Finance and Transactional Considerations

NOVEMBER 9 | European Antitrust and Other Regulatory Updates for the Automotive Industry

Presenters

Todd Liao
Shanghai
Tel. +86.21.8022.8799
todd.liao@morganlewis.com

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

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

Morgan Lewis

Contents

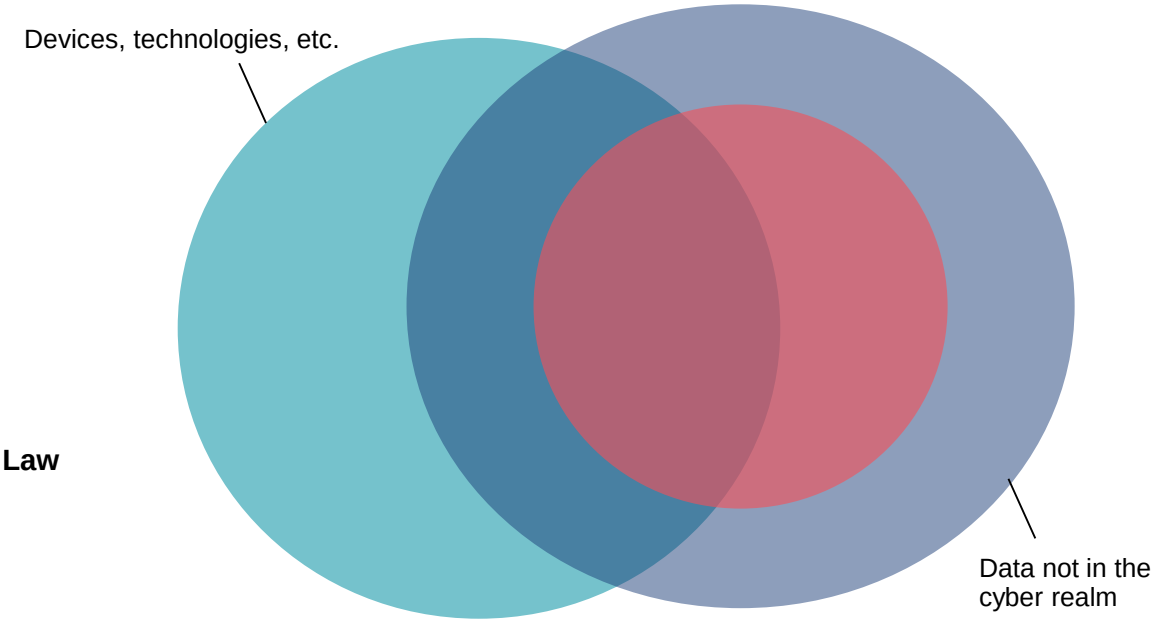
1. Overview of Legal Framework for Data Protection in China

Morgan Lewis

Legal Framework for Data Protection in China

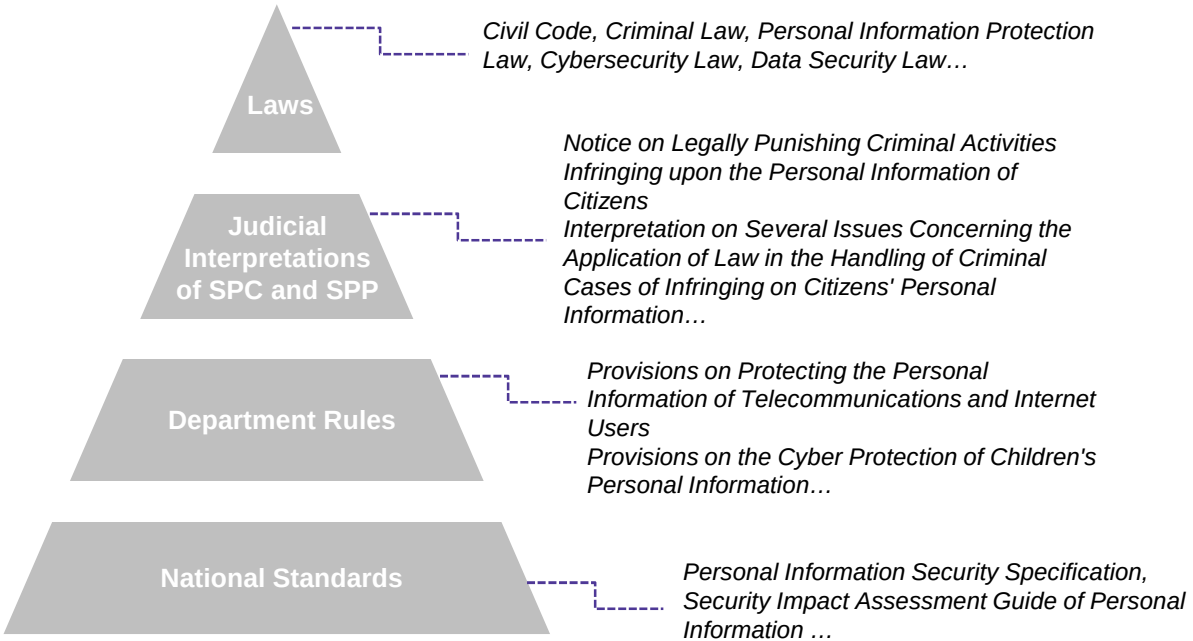
VENN DIAGRAM

- Cybersecurity Law
- Data Security Law
- Personal Information Protection Law



Legal Framework for Data Protection in China

LEGAL FRAMEWORK



Specific Rules in Automotive Sector

e.g., Provisions on the Security Management for Automotive Data (Trial Implementation)

e.g., Opinions of the Ministry of Industry and Information Technology on Strengthening the Management of Intelligent and Connected Automotive Manufacturers and Product Access

e.g., The Guide to the Development of Network Security and Data Security Standard System for Internet of Vehicles

……

2. Legislative Updates

Legislative Updates

Milestone Legislation

- Cybersecurity Law (“CSL”)
- Data Security Law (“DSL”)
- Personal Information Protection Law (“PIPL”)
- Sector-specific regulations in the automotive industry
    - Provisions on the Security Management for Automotive Data (Trial Implementation) (“Provisions”)

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

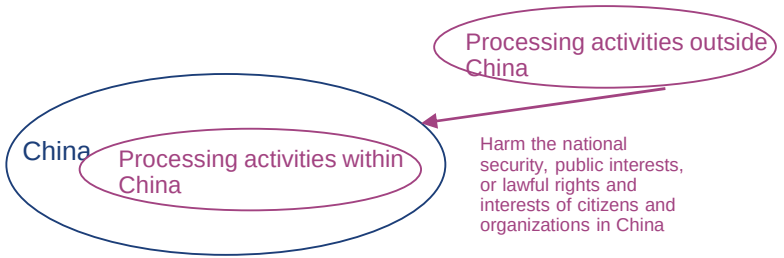
Art. 3 (2) **Data processing** includes collection, storage, use, processing, transmission, provision and disclosure of data.

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.

→ **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

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.

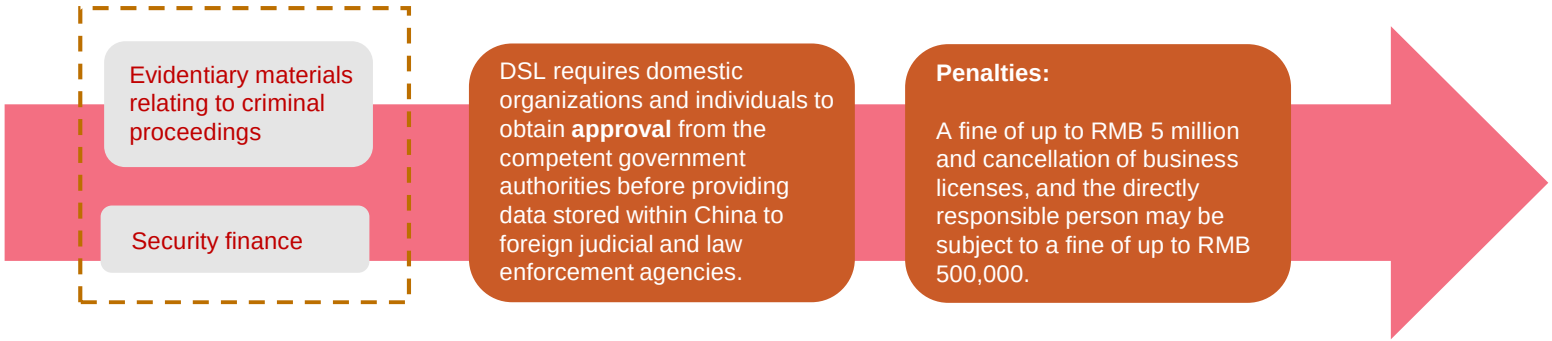
Security review decisions made according to law are final decisions.

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

Key Takeaways

Policy Framework	Review the existing policies and guidelines and make amendments to ensure compliance with relevant requirements under the DSL.
Incident Response	Establish a mechanism to deal with notification to users and authorities about data security incidents.
Trainings and Education	Provide education and training programs on data security to employees with a role in data processing, security, or compliance.
Data Operation	Check if your data is from legal and proper sources, for example, by: • clarifying the scope, purpose, method, and security measures of data collected in each business scenario if the data is directly collected by the company itself; • ensuring that there are measures to verify or commitments as to the lawfulness of data sources and keep relevant records if the data is collected and provided by others.
Classification and Categorization of Data	Monitor updates issued by sectoral authorities and local authorities on catalogues of Important Data and National Core Data and ensure that they are implemented in your classification and categorization of data.

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
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

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 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.

3. Hot Issues Affecting Automotive Industry

Morgan Lewis

Hot Issues Affecting Automotive Industry

- General Auto Data Protection Principles
- Data Localization and Cross-Border Transfer
- Requirements on Processing Important Data
- Multi-Level Protection Scheme (MLPS)

General Auto Data Protection Principles

Auto Data includes personal information and important data throughout the automotive design, manufacturing, sales, use, and operation and maintenance process. The Auto Data processors will include automobile manufacturers, parts and software suppliers, dealers, repair shops, and ride-hailing and car-sharing companies. Notably, insurance companies have been removed from the final draft.

Minimum data collection: In-vehicle processing: data should be transferred out of vehicles only when necessary; functions should not collect personal information by default, unless otherwise set by the driver before each ride; the coverage and level of definition of vehicle cameras and radars should match the requirements of the relevant functions or services, i.e. excessively broad coverage or high definition of data should be avoided; and anonymization or de-identification should be implemented whenever possible.

Driver opt-in is required for any collection of personal information during each ride. Auto Data processors must notify the users when processing personal information.

The authorities may also initiate data security assessment on processors of Auto Data when they see fit.

Data Localization and Cross-Border Transfer

Critical information infrastructure operators (CIIO)

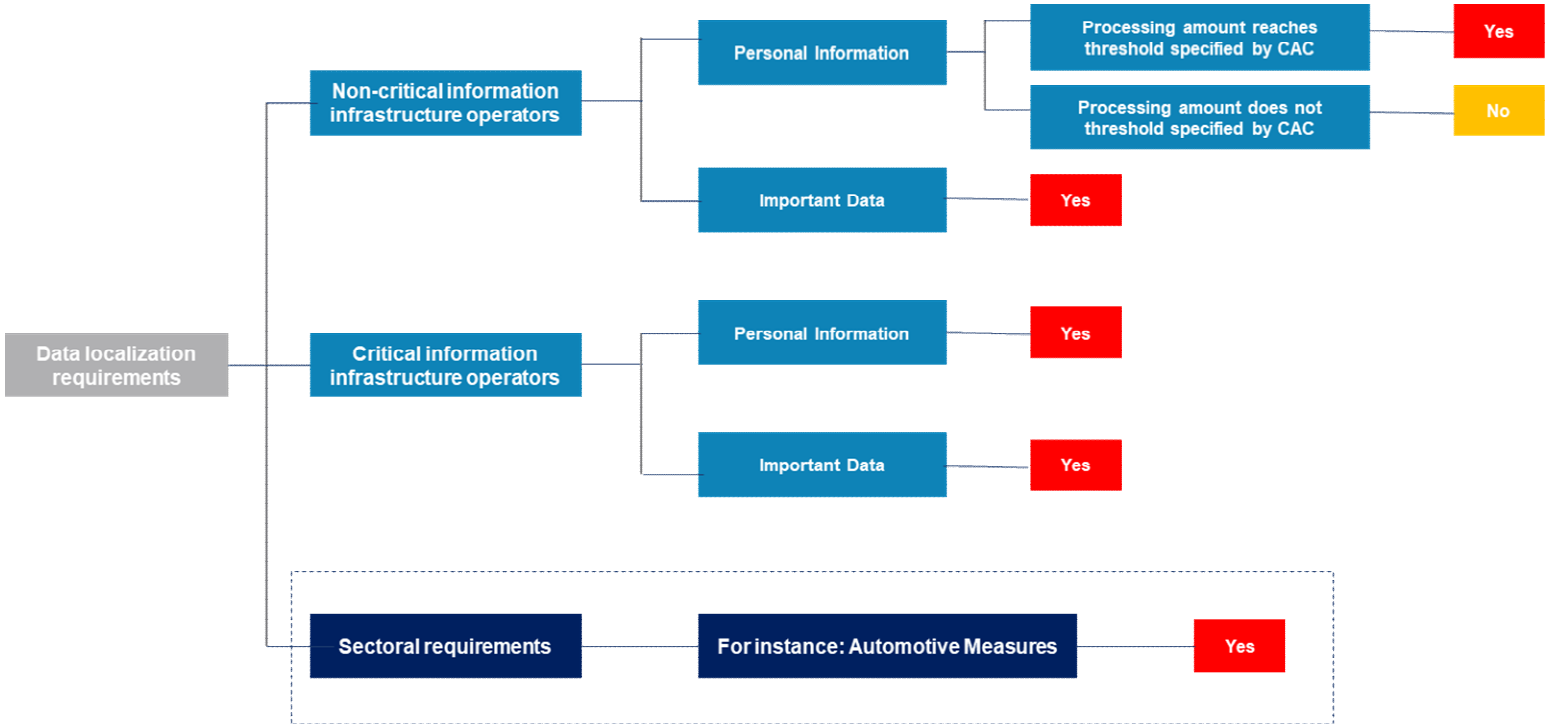
- Personal information and important data should be stored within China.
- Cross-border data transfers are subject to a government-led security assessment (and are not permitted if they bring risks to the national security, public interests, or data subjects' rights).
- Smart car manufacturer may be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

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 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 in the Automobile Industry

Important data - the data that may endanger national security, public interests or the legitimate rights and interests of individuals or organizations once such data are tampered with, damaged, disclosed, illegally obtained or illegally used, including:

- Geographic information, passenger flow, vehicle flow and other data of important sensitive areas such as military administrative zones, entities of science, technology and industry for national defense, and party and government organs at the county level or above;
- Data reflecting economic operation such as vehicle flow, logistics, etc.;
- Operational data of the automobile charging network;
- Video and image data outside vehicles that contain face information, license plate information, etc.;
- The personal information of more than 100,000 persons is involved; and
- Other data that may endanger national security, public interests or the legitimate rights and interests of individuals or organizations as determined by the CAC and the government agencies of development and reform, industry and information technology, public security and transport, etc.

Requirements for Processing Important Data by Automotive Companies

For businesses in the automobile industry collecting or generating important data during their operations in China, they are subject to the following requirements:

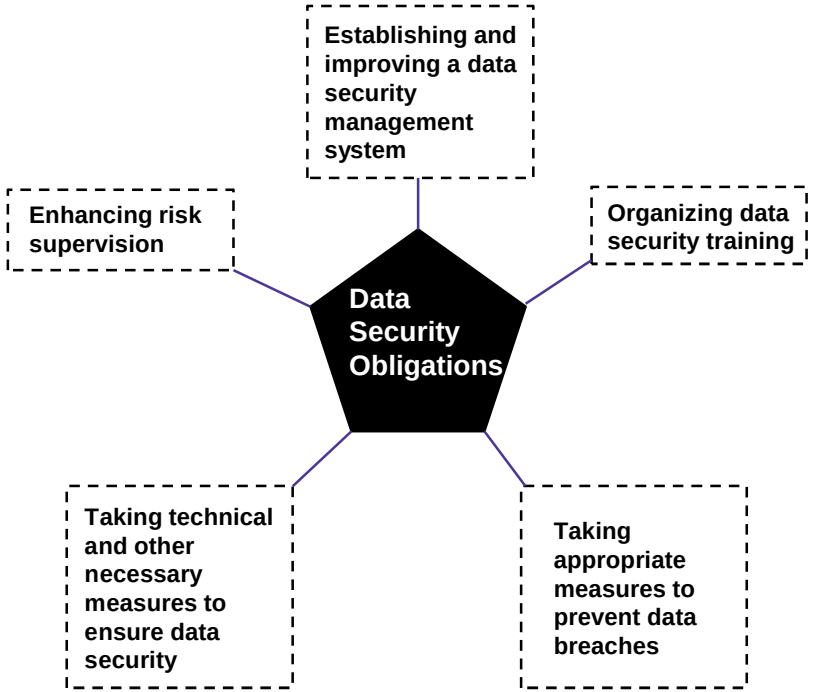
- **Data localization and restrictions on cross-border transfer** (as discussed earlier).
- **Self-risk assessment**. The *Provisions on the Security Management for Automotive Data* require automotive data handlers to conduct a risk assessment with respect to its important data processing activities, and to submit a risk assessment report to authorities.
- **Annual reporting obligation**. Prior to Dec. 15 each year, automotive data handlers processing important data are required to report a comprehensive set of information on its data management status.

Legislative Updates – Data Security Law

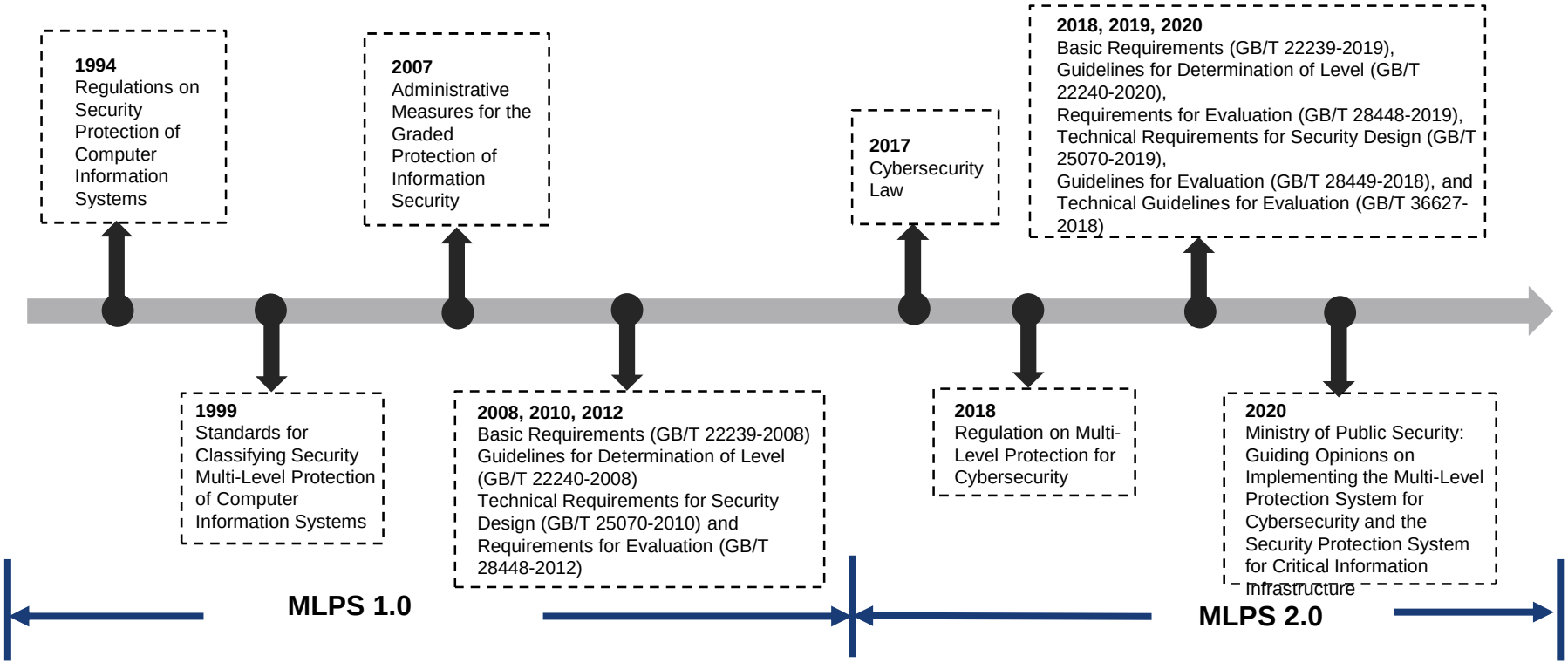
MLPS requirements and data security obligations

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.
- Article 5 of the *Provisions on the Security Management for Automotive Data* provides that companies carrying out automotive data processing activities by making use of the Internet or other information network shall implement the MLPS, strengthen the protection of automotive data, and perform the obligation of data security in accordance with the law.



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.

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.

Questions?

Todd Liao | Partner, Shanghai | todd.liao@morganlewis.com

Lesli Ligorner | Partner, Shanghai/Beijing | lesli.ligorner@morganlewis.com

Sylvia Hu | Associate, Shanghai | sylvia.hu@morganlewis.com

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.

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.

Morgan Lewis

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

Morgan Lewis