Asia Technology Innovation Series

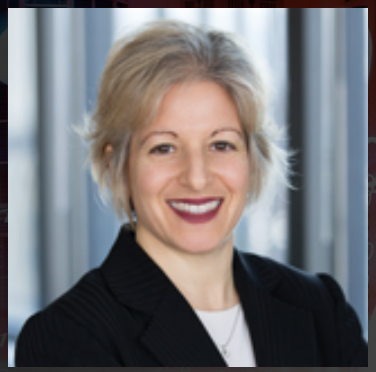
Our Inaugural Asia Technology Innovation Series features a set of tailored webinars focused on hot topics, trends, and key developments in the technology industry that are of essential importance to our friends and clients operating in Asia.

For more information:
https://www.morganlewis.com/events/asia-technology-innovation-series-2022

Morgan Lewis


Morgan Lewis
ASIA TECHNOLOGY INNOVATION SERIES
China's Privacy Regime –
What Tech Companies Need to Know
Lesli Ligorner, Todd Liao, and Sylvia Hu
Thursday, August 18, 2022
© 2022 Morgan, Lewis & Bockius LLP

Presenters



K Lesli Ligorner

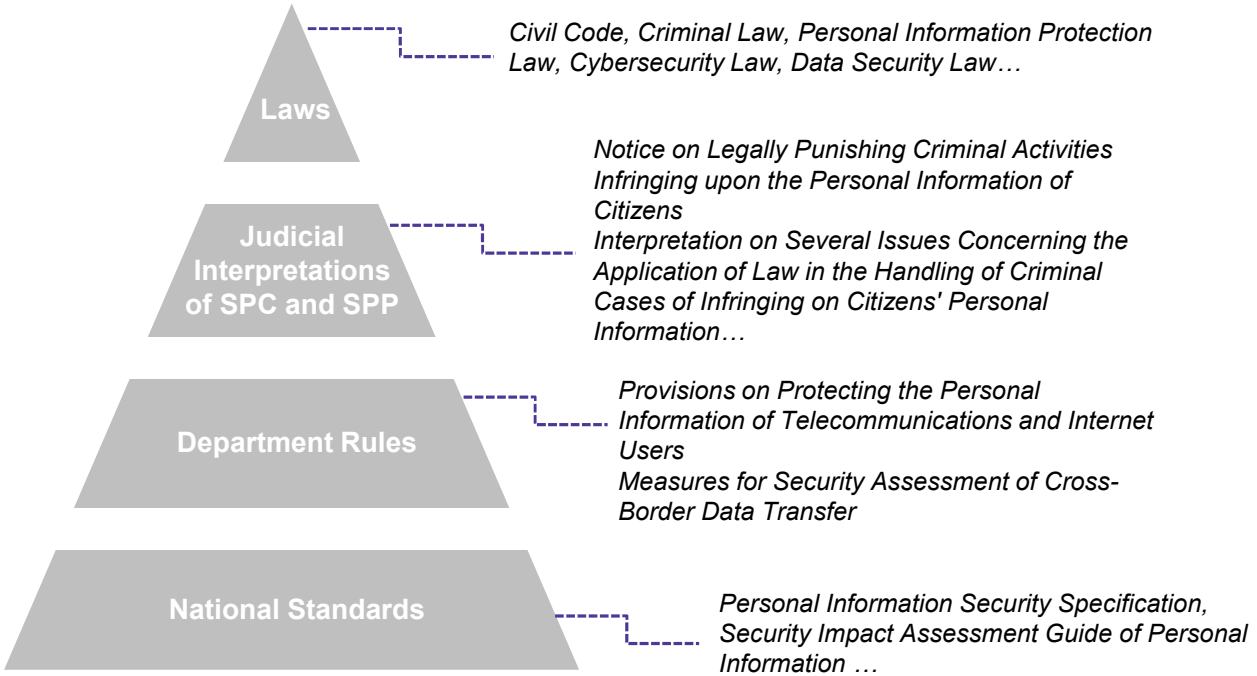
Todd Liao

Sylvia Hu

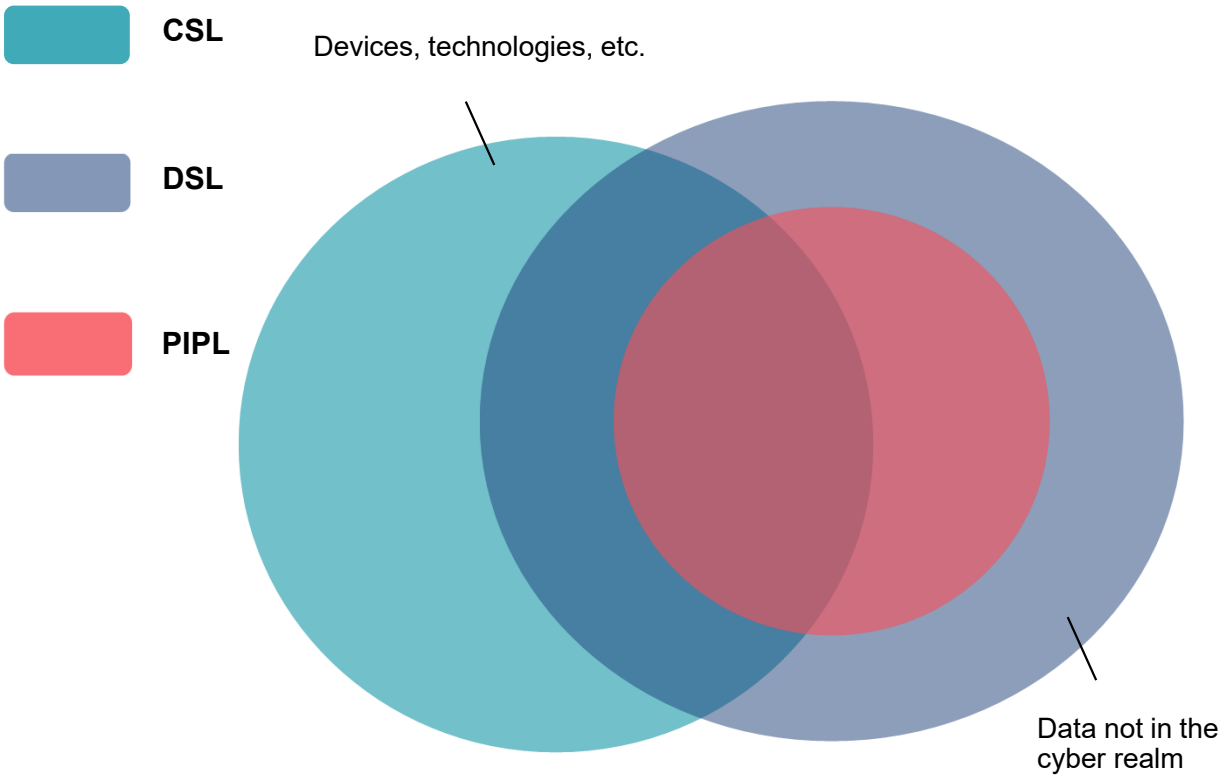
Morgan Lewis


Overview of Legal Framework for Data Protection in China
Morgan Lewis

Legal Framework for Data Protection in China



Legal Framework for Data Protection in China



Milestone Legislation

- **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

Cyber and data security obligations - Key definitions

Data categorization

DSL 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.

→ The government will publish important data catalogs

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

→ The law only provides a general principle and has not provided detailed guidance

Critical Information Infrastructure Operators (CIIO)

CSL Art. 31 CIIOs refer to operators of important network facilities and information systems in critical industries and fields which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy and the people's livelihood and public interests, including public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry.

Cyber and data security obligations - General obligations for all business operators

- The CSL, DSL and PIPL provide various technical and management measures that all business operators should take to ensure that the network is free from interference, disruption or unauthorized access, and prevent data from being disclosed, stolen or tampered:

Category	Specific Measures
Technical Measures	Taking technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity
	Taking technical measures to monitor and record network operation and cybersecurity events, and maintaining the cyber-related logs for no less than six months as required
	Taking measures such as data classification, backup and encryption of important data, etc.
Management Measures	Formulating internal security management systems and operation instructions
	Determining the persons in charge of cybersecurity and defining their accountabilities for cybersecurity
	Establishing a sound data security management system, organizing data security education and training for employees
	Formulating and organizing the implementation of emergency plans for personal information security incidents

Cyber and data security obligations - Enhanced obligations for CIIOs

- The CSL also provides enhanced technical and management measures for CIIOs, including:

Category	Specific Measures
Technical Measures	Making disaster recovery backup of important systems and databases
Management Measures	Setting up a dedicated security management body and designating a person in charge, and reviewing the security backgrounds of the responsible person and those in key positions
	Providing practitioners with regular cybersecurity education and technical training, and conducting skill assessments
	Working out an emergency plan for cybersecurity events and carrying out drills regularly

Cyber and data security obligations - Enhanced obligations for important data handlers

- Under the DSL, if business operators process important data, the following requirements will apply:

Enhanced Data Security Management

Designating persons responsible for data security and establishing data security management bodies to ensure compliance with the data security obligations

Periodical Risk Assessments

Carrying out risk assessments periodically for the data processing activities and submitting risk assessment reports to the relevant government authority

Localizing Important Data

Localizing the important data as required by laws and administrative regulations. (See details below)

Privacy obligations - Key definitions

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.

Privacy obligations - Jurisdiction

- The PIPL has an **extra-territorial effect**, which applies both to:
  - personal information processing activities within China; and
  - those that take place outside China if their purpose is to provide products or services to individuals located in China, or to analyze or assess the behaviors of individuals located in China.
- Overseas companies caught by the exterritorial jurisdiction of the PIPL should **establish a dedicated entity or appoint a representative in China** to:
  - handle matters in relation to the protection of personal information they collect
  - file the information of the entity or the representative with competent government authorities.
- Foreign organizations or individuals may be put on a "**blacklist**" .
  - The "blacklist" would restrict or prohibit them from receiving personal information from China if they infringe the personal information rights and interests of Chinese citizens or harm the national security or public interest of China.

Privacy obligations - 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.

Privacy obligations - Personal information rights

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


Hot Issues
Affecting
Multinational
Corporations
Morgan Lewis

Hot Issues Affecting MNCs

- Data Localization and Cross-Border Transfer
  - Security assessment by the government authority
  - Certification by a qualified institution
  - Standard Contract

- Multi-Level Protection Scheme (MLPS)

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
- Choose one of the following mechanisms to transfer personal information abroad
  - undergo a security assessment administered by the CAC;
  - 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 - Government security assessment

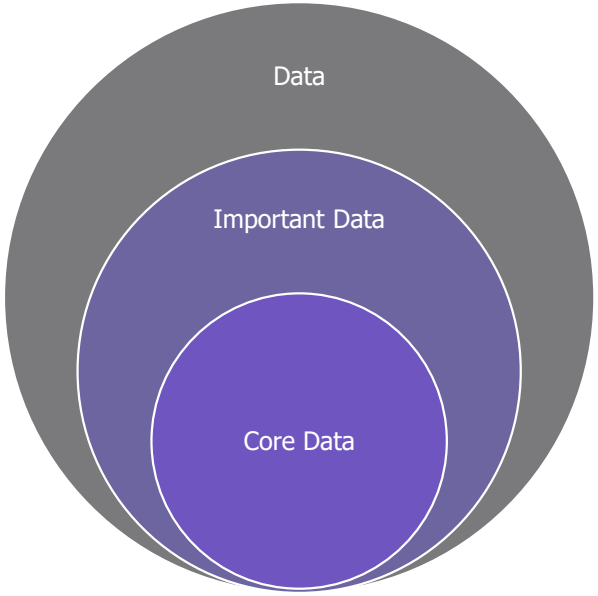
The Cyberspace Administration of China (CAC) released its long-awaited, final version of the Measures for Security Assessment of Cross-Border Data Transfer (Measures) on July 7, 2022. The Measures will take effect on September 1, 2022 and gives a grace period of six months for compliance.

Key Factors	Triggering Criteria
Based on the "**special identity**" of the data exporter (regardless of the volume involved)	Critical information infrastructure operators (CIIO)
	Operators that possess personal information of over 1 million users
Based on the "**sensitivity and scale**" of the data to be transferred abroad	The data to be transferred includes "important data"
	Since January 1 of the previous year, transferring personal information out of China that consists of (1) the personal information of more than 100,000 individuals, or (2) the sensitive personal information of more than 10,000 individuals
Other factors	Other situations to be determined by the CAC

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

Important Data - Government 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);

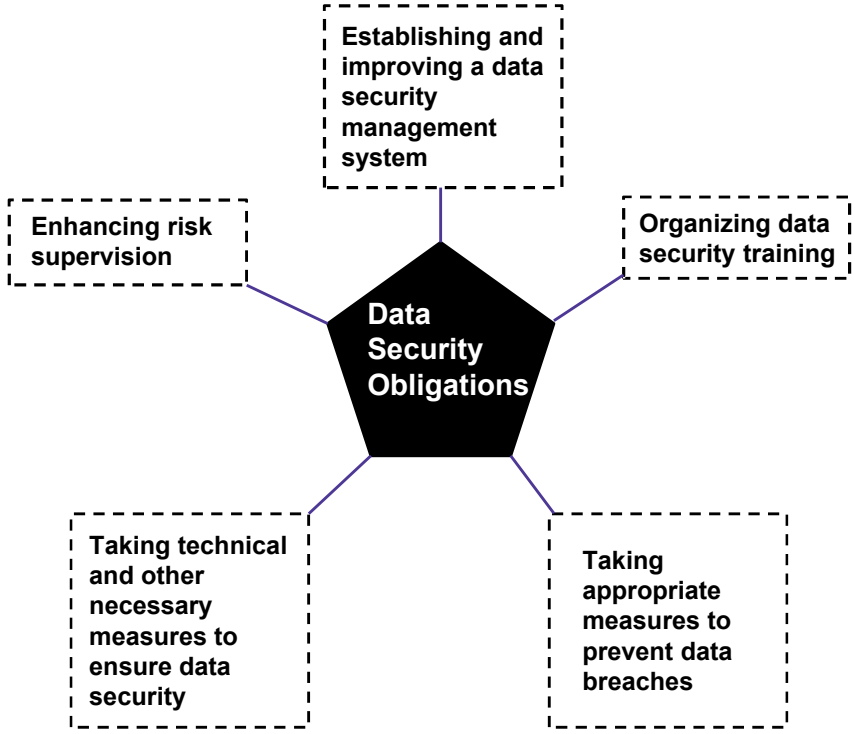
3. Data exporter should file the standard contract and the PIPIA report with the provincial competent government authority within 10 working days after the standard contract takes effect.

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

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 on 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

- 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

- **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.
- **Review and update** the current data-related policies, both internal employee notices 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?

Morgan Lewis

Next Session:
An Introduction to the Metaverse

WEBINARS

AN INTRODUCTION TO THE METAVERSE

ASIA TECHNOLOGY INNOVATION SERIES 2022

Tuesday, August 23, 2022
10:00 AM - 11:00 AM JST
09:00 AM - 10:00 AM SGT
09:00 AM - 10:00 AM CST

Register Now

Join us for a panel discussion on the metaverse—what it is, why you should be paying attention to it, and what legal issues you should be on the lookout for. This is an introductory presentation in a series on the metaverse that will delve into the legal issues that companies may face in the 3D virtual world.

OUR PARTICIPANTS

DION M. BREGMAN
PARTNER
Silicon Valley

JASON E. GETTLEMAN
PARTNER
Silicon Valley

WAI MING YAP
PARTNER
Singapore

WILLIAM HO
PARTNER
Hong Kong

For more information:
https://www.morganlewis.com/events/asia-technology-innovation-series-2022

Upcoming Sessions

August - September

Title	Date / Time	Speaker(s)
IP Year in Review: Important Chinese Cases Decided in 2021	Monday, August 29, 2022 10:00am CST/SGT | 11:00am JST	Shaobin Zhu, Lucia Tang, Jensen Xu, Bo Tang
Why Technology Companies Should Care About ESG Issues	Thursday, September 1, 2022 09:00am CST/SGT | 10:00am JST	Carl Valenstein, Karen Abesamis, Lesli Ligorner, Sin Teck Lim
Technology Disputes Involving Founders and Startup Companies in Asia	Tuesday, September 6, 2022 10:00am CST/SGT | 11:00am JST	Daniel Chia

For more information: https://www.morganlewis.com/events/asia-technology-innovation-series-2022

Morgan Lewis

Upcoming Sessions

September

Title	Date / Time	Speaker(s)
CFIUS Considerations with Foreign Investors	Tuesday, September 13, 2022 09:00am CST/SGT | 10:00am JST	Carl Valenstein, David Plotinsky
Digital Innovation and Disruption: Tech & Sourcing—The Year in Review	Wednesday, September 21, 2022 09:00am CST/SGT | 10:00am JST	Mike Pierides, Peter M. Watt Morse
Key Issues in Tech M&A	Wednesday, September 28, 2022 09:00am CST/SGT | 10:00am JST	Wai Ming Yap, Todd Liao, Shaobin Zhu, Motonori Araki, Yuting Zhu

For more information: https://www.morganlewis.com/events/asia-technology-innovation-series-2022

Morgan Lewis

Biography

K Lesli Ligorner
Partner
Shanghai
lesli.ligorner@morganlewis.com

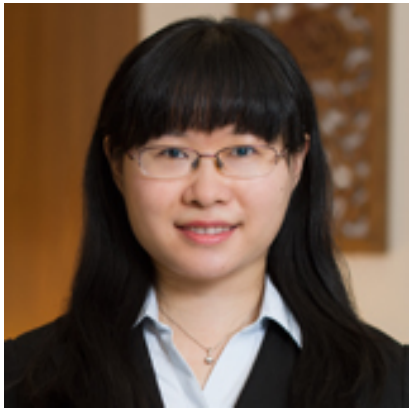
K Lesli Ligorner has more than 20 years of experience serving clients on a wide range of labor and employment matters, with 15+ of those years spent on the ground in China. She has been advising a broad range of financial services; telecommunications, media, and technology; life sciences; and general 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.

Biography

Todd Liao
International Partner
Shanghai
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.

Biography



Sylvia Hu
Associate
Shanghai
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.


Stay up to date:
US-China Trading Policy & Global Impact
Make sure to check out our US-China Trade Policy and Global Impact web-page for all of our latest content:
https://www.morganlewis.com/topics/us-china-trading-policy-global-impact

THANK YOU