LEGAL ISSUES OF CSL, DSL AND PIPL

CYBERSECURITY & DATA COMPLIANCE

China's Data Protection Laws: CSL / DSL / PIPL

Cyber Security Law

Effective date: June 1, 2017

- Protects national security and safeguards cyberspace sovereignty
- Cybersecurity obligations (DPO & MLPS)
  - Ordinary network operators
  - Critical Information Infrastructure (CII) operators
- Rules of data localization and export
- Personal information protection rules

Data Security Law

Effective date: Sept 1, 2021

- Protects national security
- Extraterritorial effect on offshore entities
- Excludes state secret nor military related data, but introduces new category of "State Core Data"
- Rules of "Important Data" security, localization and export
- Establishes data security review system on data processing activities endangering national security

Personal Information Protection Law

Effective date: Nov 1, 2021

- Protects rights and interests of personal information subjects
- Extraterritorial effect on offshore entities
- First over-arching national law governing full life circle of personal information processing
- Introduces rules on personal information localization and export

Cyber Security Law

- **Effective date:** June 1, 2017
- **Enforcement agencies:** Cyberspace Administration of China ('CAC')
- **Data localization and cross border transfer**
  - > Personal information and important data collected in China by CIIOs must be stored within China.
  - > Security assessment should be conducted by CIIOs prior to providing personal information and important data abroad.

Data Security Law

- **Effective date:** Sept 1, 2021
- **Enforcement agencies:** CAC
- **Data localization and cross border transfer**
  - **Important data**
    - > Except for CIIOs, the DSL expands the requirement of important data compliance to all businesses that process important data. These requirements are not yet defined.
    - > Local governments and regulatory agencies are required to develop more detailed catalogues to identify the scope of “important data” based on their respective regions and industry sectors.
    - > The CAC and other regulatory agencies have yet to formulate cross-border transfer rules of important data for non-CIIOs.
  - **Restrictions to provide and transfer data to overseas law enforcement agencies**
    - > Governmental reporting is required, and mandatory approval is needed.

Personal Information Protection Law

- **Effective date:** Nov 1, 2021
- **Enforcement agencies:** CAC
- **Data localization and cross border transfer**
  - > CIIOs and entities that process personal information exceeding the prescribed threshold (yet to be determined) should locally store personal information and conduct government-led data cross-border transfer review.
  - > Data processors other than CIIOs or the entities are basically free to transfer personal information abroad. Such processors should enter into a standard contract formulated by the CAC with the personal information recipient or get certified by designated agencies.
  - > Personal information processers must seek approval from competent authorities before providing personal information stored in China to any foreign judicial or law enforcement authority.

Key Points in Data Security and Privacy Compliance

Personal information security and protection

- Full life-cycle management and protection for personal information in data collection, processing, storage and deletion
- Conducting personal information protection impact assessment under several specified circumstances.
- Regularly conducting compliance audits on its personal information processing activities.
- Other general security obligations include: formulating internal management systems and operating procedures; taking technical security measures such as encryption and de-identification; reasonably determining the authority to access and process personal information and conducting security education and training for relevant employees on a regular basis.

Data security obligations

- Establishing comprehensive data security management systems, organizing data security trainings, and implementing necessary measures to ensure data security.
- For important data, appointing data management teams and data security officers, and regularly conducting and reporting on risk assessments of data activities.
- Strengthening risk monitoring, taking remedial actions when data security defects or loopholes are detected, and notifying users and authorities of security incidents.
- Cooperating with the public security and national security authorities in retrieving data for the purpose of safeguarding national security or investigating crimes.

Key Points in Data Security and Privacy Compliance

Cyber security multi-level protection scheme (MLPS)

> Taking measures such as data classification, important data backup and encryption.
> Taking technical measures to prevent computer virus, 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 at least six months.

Data localization and cross border transfer

> Personal information and important data collected in China by CIIOs must be stored within China.
> Security assessment should be conducted by CIIOs prior to providing personal information and important data abroad.
> Data processors other than CIIOs or the entities are basically free to transfer personal information abroad. Such processors should enter into a standard contract formulated by the CAC with the personal information recipient or get certified by designated agencies.
> Personal information processers must seek approval from competent authorities before providing personal information stored in China to any foreign judicial or law enforcement authority.

Liability and Penalty

- **CIIO:**
  - **using products and/or services which have not undergo or have failed in the security review**: prohibition of use; fine.
  - **unlawfully providing important data overseas**: warning and making corrections; fine; winding up for rectification, shutdown of website, and revocation of business license.
  - **storing or providing network data out abroad**: warning and making corrections; fine; winding up for rectification, shutdown of website, and revocation of business license.
  - administrative punishment according to public security regulations;
  - criminal liability.

- **Data processor (when performing the obligation of protecting personal information):**
  - warning and making corrections; suspending or terminating the provision of services; fine.
  - liability for damages and other tort liabilities.
  - administrative punishment according to public security regulations;
  - criminal liability.

David Pan

Tell: +86 21 3135 8701

+86 136 2172 0830

Email: david.pan@llinkslaw.com

- Dr. David Pan is the head partner of Corporate Compliance Service Group. Dr. Pan obtained his LL.M. from Harvard Law School, and his Doctor of Jurisprudence from Shanghai Jiao Tong University. Dr. Pan was admitted to practice law in 2002. He is also admitted in New York State, USA.

- Dr. David Pan has practiced law in China and in the U.S. over 20 years. He accumulated an in-depth knowledge on Chinese and international business culture and legal systems. Before joining Llinks, Dr. Pan worked in two well-known Chinese law firms, and most recently worked for a Fortune 500 Company as its General Counsel for Greater China. In addition to his corporate services such as mergers and acquisitions, joint venture, technology license etc., Dr. Pan specializes in various compliance matters including anti-trust, anti-corruption, cybersecurity and data protection, export control and sanctions. The clients that he represented spread over various industries, including auto, investment, energy, pharmaceutical, chemical, medical, food, advanced manufacturing, sports and entertainment, retail and consumer, real estate.

- Based on his thorough understanding on business operations, Dr. Pan also specializes in providing companies with practical solution-oriented services in the regulatory compliance areas of anti-corruption, antitrust, and anti-unfair competition.

- In the early 2000s, Dr. Pan started to represent MNCs in data and cybersecurity related legal matters, such as offshore server, log records storage and filing, personal data collection and use, data integrity, centralized data process, differentiation between trade secrets and state secrets etc. In the course of handling these cases, Dr. Pan gained solid practical experiences in this field. Dr. Pan has served clients in healthcare, auto, tourism, e-commerce, retail, education, services, finance, fintech, and manufacturing in the establishment and improvement of compliance system in the entire process of data collection, storage, usage, transfer, and destruction, and provided compliance solutions for cyber security, digital transformation, and big data.

- Dr. Pan is recommended as top lawyers in fields of cybersecurity and data, corporate, compliance, antitrust and competition by rating agencies like ALB, Chambers, Legal 500, LEGALBAND, Who's Who Legal. Dr. Pan acts as an adjunct professor in Law School of Shanghai Jiao Tong University and an examiner expert of Shanghai United Assets and Equity Exchange.