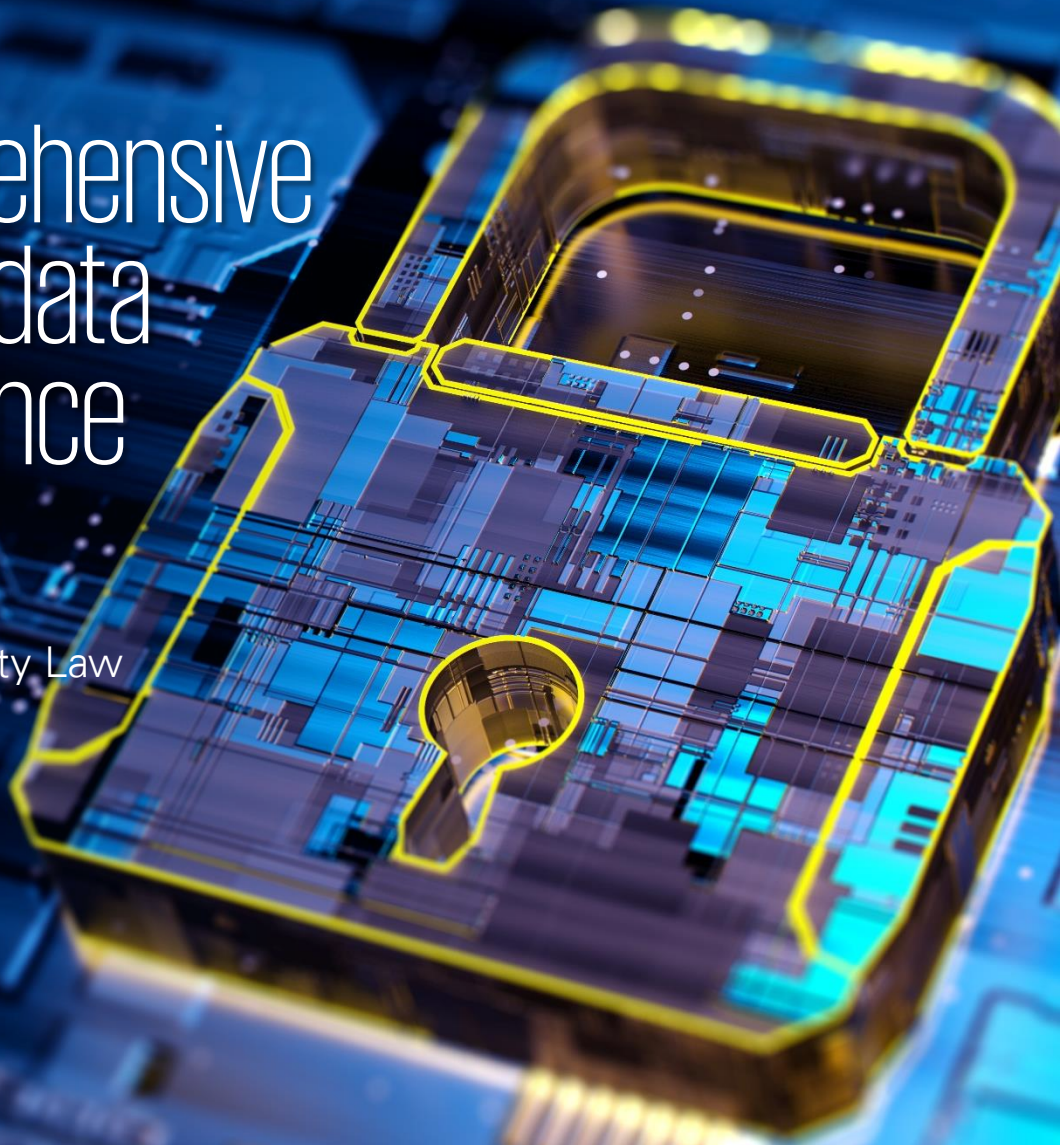
KPMG

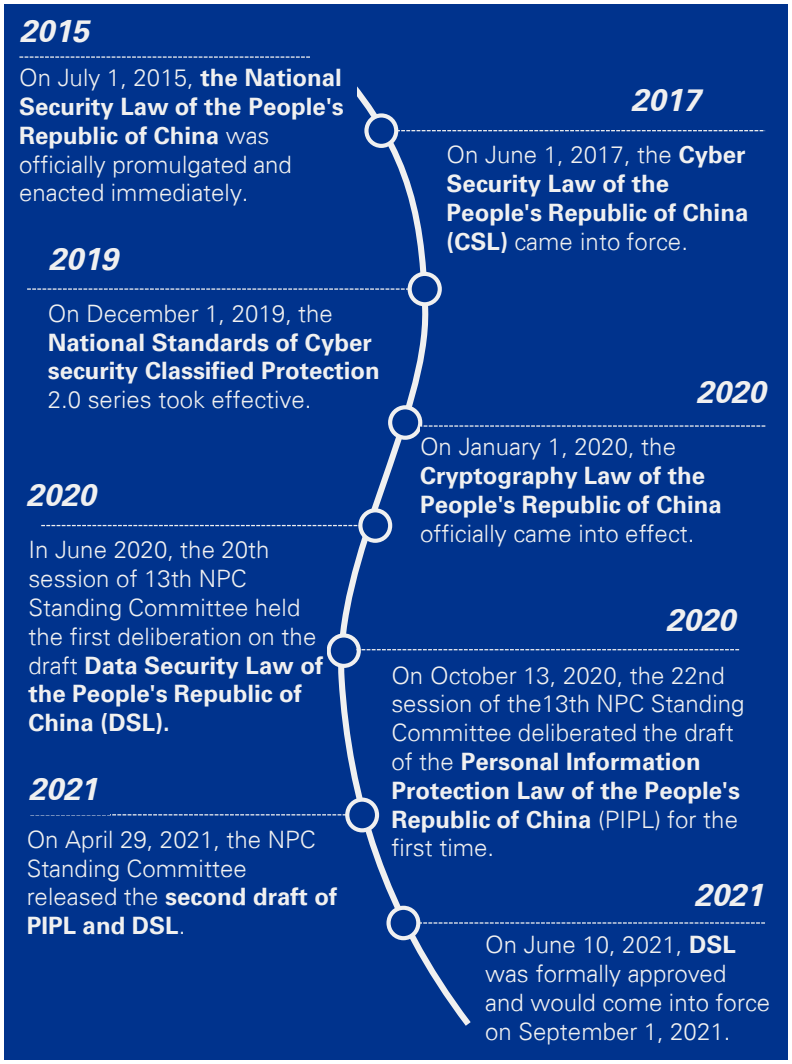
# Establishing comprehensive cyber security and data protection governance system

Quick summary of China Data Security Law and recommendation on next actions



kpmg.com/cn

# Building the depth and boundary of security governance through DSL and CSL




On July 1, 2015, the **National Security Law of the People's Republic of China** was officially promulgated and enacted immediately, within which cyber security and data security were clearly included as part of state security.

On June 1, 2017, the **Cyber Security Law of the People's Republic of China (CSL)** came into force, which stipulates the obligations and requirements of security management related to the construction, operation, maintenance and use of the network within the territory of PRC, as well as the supervision and management of cyber security.

On June 10, 2021, the **Data Security Law of the People's Republic of China (DSL)** was officially promulgated and would come into effect on September 1, 2021. DSL regulates data processing activities and safety supervision within the territory of PRC. It also mentions that for data processing activity outside PRC, if it is harming national security, public interests or the legitimate rights and interests of citizens and organizations of PRC, legal responsibility is to be pursued in accordance with law. The upcoming Personal Information Protection Law of the People's Republic of China (PIPL) will then supplement detail processing and protection requirements for personal information as a specific type of data.

In the next 6-12 months, it is recommended to key monitoring the evolving regulatory landscape, especially for the following relevant laws, regulations and supporting standards:

- **Data security management regulations**
- **Important data catalog**
- **Cross-border transfer security assessment regulations for Important Data**
- **Critical information infrastructure protection regulations**
- **Cyber security classified protection regulations**
- **Cross-border transfer security assessment regulations for Personal information**

# DSL highlights

## Applicable scope

1

- Data processing activities and security supervision within the territory of PRC; and data processing activities outside the territory of PRC that harms the national security of the P.R.C., the public interest, or the lawful rights and interests of citizens and organizations, are to be pursued for legal responsibility in accordance with law.
- "Data" as used in this Law refers to any record of information in electronic or other forms

## Policy system

2

- Regulations for data classification and categorization protection, important data protection and state core data protection
- Data security risk management, monitoring and alerting mechanism
- Data security emergency response mechanism
- Data security review regulation
- Data export control regulation

## Competent authority

3

- Central leading group of national security
- All districts and departments
- Industrial regulators (Manufacturing, Telecom, Transportation, Finance, Natural Resource, Education, Science and Technology, etc.)
- Public security organs, National security organs,
- State cyberspace administration organs
- State Council departments in charge of standardization and other relevant State Council departments

## Protection obligations

4

- Data processing activities should be legal and legitimate, and in line with social morality and ethics
- Establish and enhance the full lifecycle of data security management, organize and perform data security awareness training, and take relevant technical measures and other necessary measures to ensure data security; protect data based on MLPS for data processing activities utilizing Internet; Strengthen risk monitoring and emergency response
- Important data processors should assign data security officer and organization, perform risk assessment and report to authority regularly, and manage cross-border transfer appropriately

## Legal responsibility

5

- Warning and mandated rectifications
- Fines:
  - Organization: RMB 50,000 ~ 10 million
  - Individual: RMB 10,000 ~ 1 million
- Suspend relevant business, suspend business for rectification, revoke relevant business license
- Others: To investigate criminal responsibility, to bear civil responsibility, and to punish public security administration according to law

# Classified data protection

Data Security Law

Article 6 …Sector competent authorities, including Industry, Telecommunication, Transportation, Finance, Natural Resources, Healthcare, Education, Science and Technology etc., are to undertake data security regulatory duties in the corresponding sector…

Article 21 The state is to establish a categorical and hierarchical system for data protection and carry out categorized and graded data protections based on the importance of the data in economic and social development as well as the extent of harm to national security, the public interest. The national data security coordination mechanism coordinates the relevant departments to determine catalogue of important data and strengthen protections of the important data.

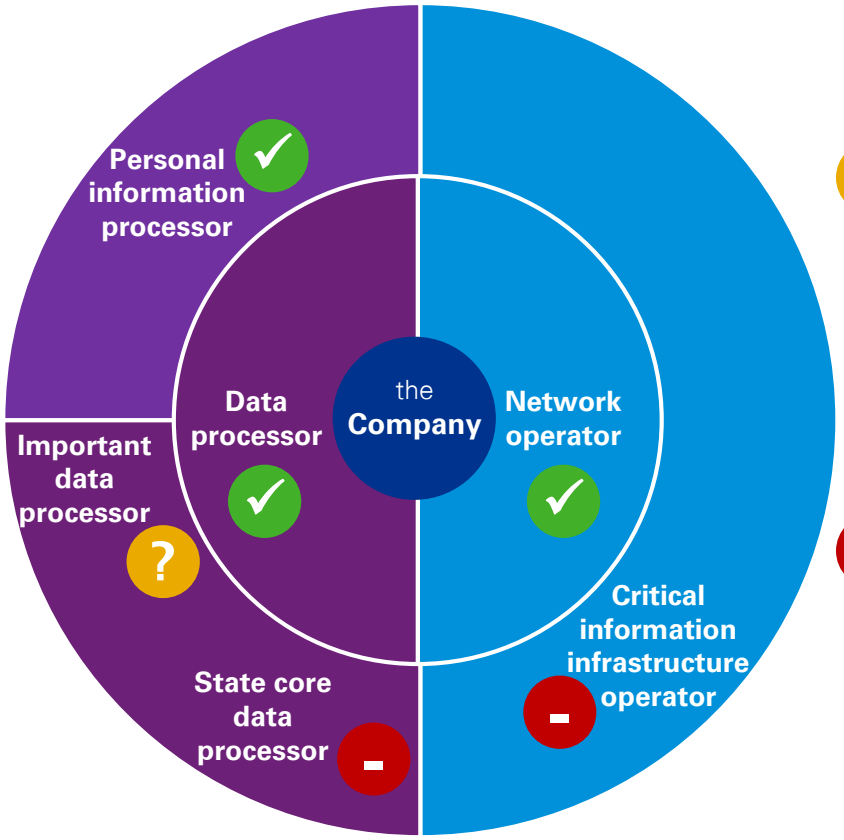
Data related to national security, the lifeblood of the national economy, important people's livelihood, major public interests and others belong to the national core data, shall apply to a more stringent management system.

Each region and department shall determine the catalogue of important data within that region and department and corresponding industries and sectors on the basis of the categorical and hierarchical protection system, and conduct key protection for data entered in the catalogue.

- Data classification is the foundation of data security management. Existing internal data classification policy and approach might need to be adapted and optimized in the future to address the state data classification protection policy system.
- Important data catalog and detail list are yet to be defined and clarified. Thus, it is suggest to keep monitoring further notice especially from relevant sector competent authorities.

| Industry | Telecommunication | Transportation | Finance | Natural Resources | Healthcare | Education | Science and Technology |
|---|---|---|---|---|---|---|---|
| Ministry of Industry and Information Technology | | Ministry of Transport | The People's Bank Of China | Ministry of Natural Resources | National Health Commission | Ministry of Education | Ministry of Science and Technology |
| Guidelines for Classification and Classification of Industrial Data (Trial) (2020) | | Financial data security-Guidelines for data security classification(JR/T0197—2020) | | Information security technology-Guide for health data security（GB/T 39725-2020） | | Regulations of the People's Republic of China on the Administration of Human Genetic Resources (2019) | |

# Understanding different roles of a Company in cybersecurity and data protection




✓ Companies basically would be considered as **network operators** (CSL), **data processors** (DSL) **and personal information processors** (PIPL draft)

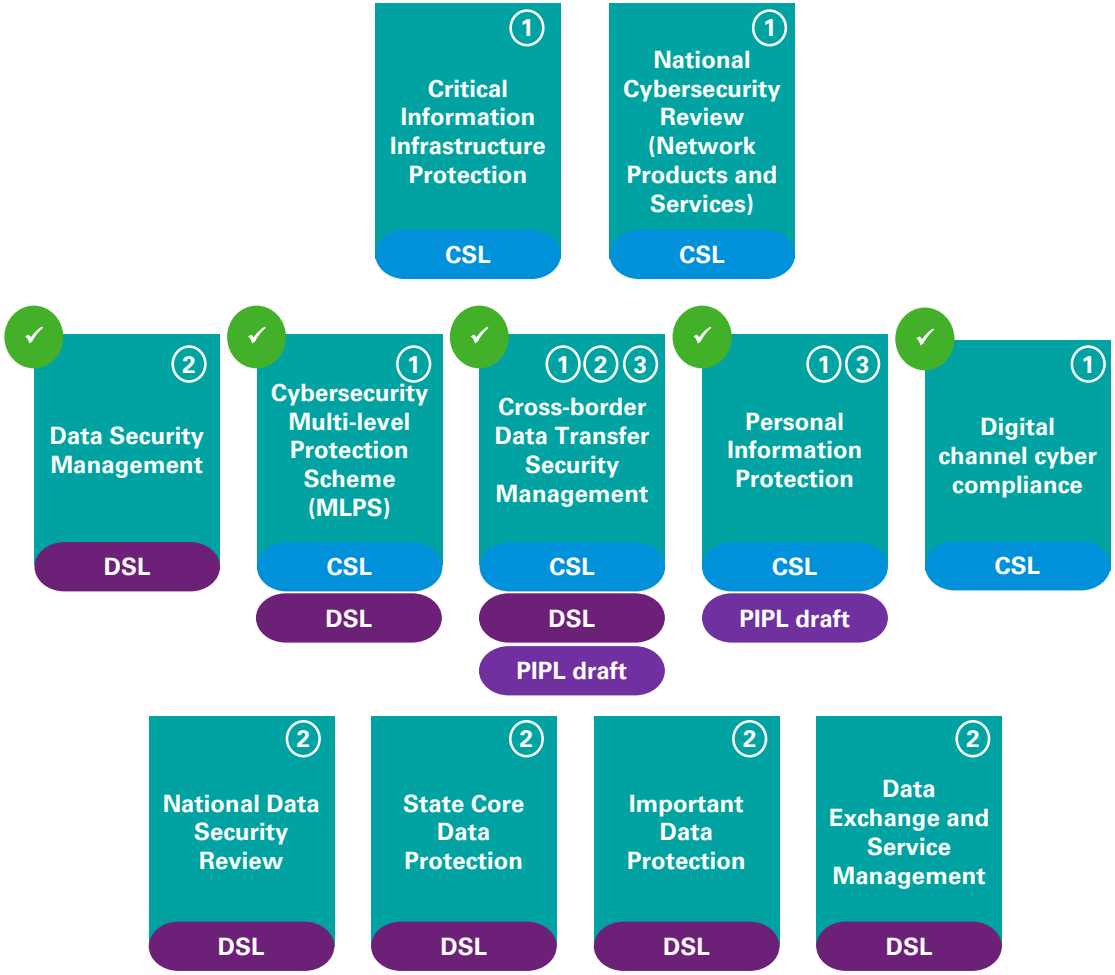
? Some companies may be involved in the processing of important data

- ✓ State data security coordination mechanism coordinates the relevant departments to define important data catalogue.
- ✓ Each region and department shall determine the detail catalogue of important data within that region and department and corresponding industries and sectors according to the classified data protection policy system.

– Limited companies may be involved in the processing of state core data and/or operate critical information infrastructure

- ✓ Data related to national security, the key for the national economy, important people's livelihood, major public interests and others belong to the national core data.
- ✓ The critical information infrastructure that, once it is destroyed, loses its functionalities or encounters data leaks, may greatly harm national security, the national economy, the people's livelihood and the public interest.

# Extended cybersecurity and data protection obligations




To address basic compliance requirements, Companies shall establish and improve the following:

1. Information Security Management System
2. Data Security Management System; and
3. Personal Information Management System

**Possible external compliance activities**

- MLPS filing, assessment & certification
- Data security assessment & certification
- Personal information protection assessment & certification
- Submit the name & contact information of the person responsible for personal information protection
- personal information and important data cross-border transfer security assessment
- Report cyber security events
- Report data security events
- Report personal information security incidents

# Impact to existing cybersecurity and data protection governance framework

Implement full **LIFECYCLE DATA SECURITY MANAGEMENT**. Previously pure technical or isolated management approach should be systematically analyzed and re-engineered, and shall integrate with Companies' digital transformation, data governance and operation management, taking a top-down and collaborated approach to achieve effective and implementable security governance.

**PROTECT CYBERSPACE AND DATA**. DSL aims for the full set of data while draft PIPL aims to protect a specific type; CSL sets requirements based on traditional information security management framework but from cyberspace security protection perspective. According to business and technology operation and data processing scope, Companies shall make sure existing information security management system, data security management system and personal information management system can effectively integrate and extend to address law level cybersecurity and data protection requirements in China.

**DATA LOCALIZATION AND CROSS-BORDER TRANSFER SECURITY MANAGEMENT**. According to CSL, DSL and draft PIPL, localized processing personal information (reaches certain volume) and important data is now extended to all processors but not only critical information infrastructure operators. Companies will then need to consider how to develop appropriate localization strategy, and to manage cross-border data transfer as part of the full lifecycle data security management activities.

**LOCALIZING NOT ONLY DATA AND INFORMATION SYSTEM**. Personnel "localization" is also necessary, for example, Companies should at least assign a cybersecurity person in charge locally in China, while personal information protection officer, data security officer and cybersecurity, data security and personal information protection organizations shall be assigned if applicable. Besides, along with the localization of data and information system, localization of operational teams, procedures and tools shall also be established and operated, with certain integration and interaction with existing global framework.

# KPMG cybersecurity and data protection service

**Globalized cybersecurity and legal professional teams**

**Rich experience in cybersecurity and data protection planning and implementation**

**Strong connection and cooperation in local cyber eco-system**

**Technical solutions that can be customized and sustained**

# Contact us


**Henry Shek**
KPMG China
Cybersecurity Advisory
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

**Richard Zhang**
KPMG China
Cybersecurity Advisory
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

**Brian Cheung**
KPMG China
Cybersecurity Advisory
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

**Quin Huang**
KPMG China
Cybersecurity Advisory
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

**Danny Hao**
KPMG China
Cybersecurity Advisory
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com


**kpmg.com/socialmedia**