# Data security: Safeguarding High-quality Development of the Digital Economy

<Regulation for the Administration of Network Data Security> is finalised and will take effect January 1, 2025

October 2024

# Enhancement of data security capabilities is a fundamental compliance obligation and a timely move to maintain competitiveness in the digital era

"Enhance data security capabilities, establish a fundamental system for data classification and grading protection, and improve the work system for network data monitoring, early warning, and emergency response."

- <Overall Planning for the Development of Digital China>, 2023, by the Central Committee of the Communist Party of China and the State Council

## Strengthening data security capabilities is a fundamental compliance obligation

Data security management is undergoing a shift from reactive legislation to proactive practice. Regulatory frameworks for personal information protection have become increasingly comprehensive, promoting the standardisation and systematisation of data security practices. The identification and protection of sensitive data, as well as the exploration of flexible cross-border data transfer regulatory mechanisms, are also advancing. Businesses must remain vigilant to ensure ongoing compliance.

## Data security bolsters technological innovation

As emerging technologies such as big data, artificial intelligence, and blockchain become more widely adopted, new security challenges emerge. To enable seamless technological innovation, enterprises must continuously upgrade their security measures with close attention to data security to identify and respond to potential risks.

## Data protection safeguards business competitiveness

An organisation's data contains valuable trade secrets, customer information and market insights. Securing the confidentiality of this data directly impacts the business stability and market competitiveness of enterprises. Only by prioritising data security management, integrity and access control can enterprises thrive in dynamic market conditions and achieve sustainable growth.

# The Regulation for the Administration of Network Data Security (the Regulation) is the first regulation by the State Council under the China CSL, DSL and PIPL

**2015**

On July 1, the **State Security Law of the People's Republic of China** was officially promulgated and came into force.

**2017**

On June 1, the Cyber Security Law of the People's Republic of China (CSL) officially took effect.

**2019**

In May, the Cyberspace Administration of China publicly solicited comments on the Administrative Measures on Data Security (Exposure Draft).

**2021**

On September 1, the Data Security Law of the People's Republic of China (DSL) officially came into effect.

**2021**

On November 1, the Personal Information Protection Law of the People's Republic of China(PIPL) officially came into effect.

**2021**

On November 1, the Cyberspace Administration of China publicly solicited comments on the Regulation for the Administration of Network Data Security (Exposure Draft).

**2024**

On August 30, the State Council executive meeting reviewed and approved the Regulation for the Administration of Network Data Security (Draft).

**2024**

**On September 1, the Regulation was released and will be enacted from January 1, 2025.**

As of September 2024, various industry regulatory authorities, including the Ministry of Industry and Information Technology, the People's Bank of China, and the Ministry of Education, have issued data security-related management measures for industry sectors like industry and information technology, finance, education, telecommunications, and the automotive.

## Applicable scope

- Network data processing activities conducted online within China, as well as the supervision and management of network data security.
- Personal information processing activities conducted outside of the country that fall under the scope stipulated under PIPL Article 3.
- Network data processing activities conducted outside of the country but damage the national security of the People's Republic of China, public interests, or the legitimate rights and interests of citizens or organisations.
- This regulation does not apply to personal or household data processing activities carried out by individuals for personal or family purposes.

## Key focus

### General provisions

- Data Security Strategy and Governance
- Data Security Lifecycle Management
- Data Security Management Framework
- Data Security Technology and Operation

### Special processing activities

- National security review
- Personal information protection
- Key data management
- Cross-border data transfer management
- Network platform service provider management

## Consequences of non-compliance

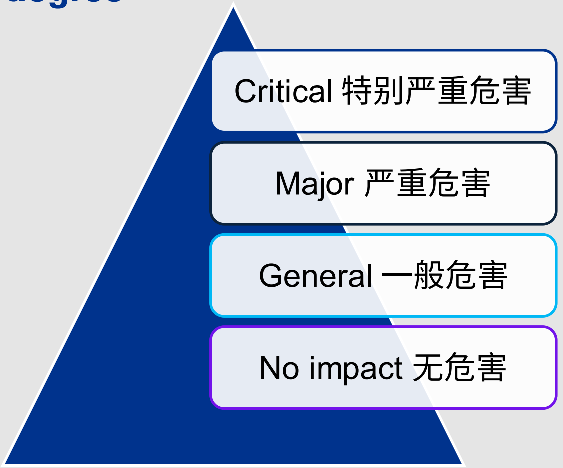
- Generally refers to CSL, DSL and PIPL, with more details provided if violating requirements under general provisions, national security review or key data security management:
  - ❑ Fines (up to RMB 10 million for an organisation; up to RMB 1 million for directly responsible supervisors and other responsible personnel)
  - ❑ Rectification, warnings, illegal gains confiscated, suspension for rectification, revoke of licenses, etc.

# Data security governance begins with Data Classification

## Impacted object

- National Security
- Public Interest
- Social Order
- Economic Operation
- Individual Rights
- Organisational Rights

## Impact degree



Given the importance of data in economic and social development as well as the severity of harm caused by incidents like data leaks, tampering, destruction, or the illegal access, use, or sharing, data is classified into three levels: core data, key data, and general data. General data is further categorised into four sub-levels (1 to 4) depending on the scope and severity of any potential impact.

| Data Security Classification | Data Security Levels | Data Classification Criteria | |
|---|---|---|---|
| | | Impacted object | Impact degree |
| **General data** | **Level 1** | Individual Rights, Organisational Rights | No impact |
| | **Level 2** | Individual Rights, Organisational Rights | General |
| | **Level 3** | Individual Rights, Organisational Rights | Major |
| | **Level 4** | Individual Rights, Organisational Rights | Critical |
| | | Economic Operation, Social Order, Public Interest | General |
| **Key data** | | Economic Operation, Social Order, Public Interest | Major |
| | | National Security | General |
| **Core data** | | Economic Operation, Social Order, Public Interest | Critical |
| | | National Security | Critical or Major |

References: GB/T 43697-2024 Data Security Technology – Rules for data classification and grading.

# Network data processors should focus on enhancing data security governance

## Data Security Strategy and Governance

- Generally includes developing a **data security strategy, outlining principles for data classification and protection**, and implementing processes for managing **data security risk and ensuring compliance**.
- Specifically, in terms of **data classification** and **compliance supervision**, the Regulation specifies that:
  - Data must be classified and managed accordingly.
  - Network data processors are responsible for the security of the data they handle and shall establish comprehensive data security management systems and technical protection mechanisms.
  - Network data processors shall cooperate with relevant authorities conducting lawful supervision and inspection of their network data security practices.

## Data Security Lifecycle Management

- Generally includes **security controls for data collection**, **transmission**, **storage**, **usage**, **exchange and sharing**, **and destruction or disposal**.
- Specifically related to **data collection security** and **data usage security,** the Regulation specifies that:
  - When using automated tools to access and collect data, network data processors must assess the impact on network service performance and functionality. Collection methods must not interfere with normal network service operations.
  - When providing services to state agencies or CII operators, or participating in the construction, operation, or maintenance of other public infrastructure or service systems, network data must not be processed without the consent of the entrusting party. Correlation analysis of network data is also prohibited without consent.

## Data Security Management Framework

- Generally includes **data security organisation**, **personnel competency**, **policies and procedures**, and **key measures and evaluation management**.
- Specifically, in terms of **data security emergency response and complaint handling procedures**, the Regulation specifies that network data processors shall:
  - Establish and enhance emergency response plans for network data security incidents, report to the relevant authorities according to regulations, and notify interested parties.
  - Accept public supervision by establishing convenient channels for network data security complaints and reports, publicise information on complaint and report channels, and promptly accept and handle network data security complaints and reports.

## Data Security Technology and Operation

- Generally includes **data security identification**, **protection**, **monitoring**, and **response technologies**.
- In addition to classified protection measures **regarding encryption**, **backup**, **access control**, **vulnerability management**, and **authentication**, the Regulation specifies that:
  - Based on cyber security classified protection ("MLPS"), necessary technical measures must be adopted to ensure data encryption, backup, access control, security authentication, and others to protect network data and prevent illegal and criminal activities targeting or exploiting network data.
  - In response to security flaws, vulnerabilities, or risks, remedial measures should be taken immediately with adequate reporting and communication. If a risk involves national security or public interest, a report must be submitted to the relevant authorities within 24 hours.

# Requirements for special processing activities

## Focus on integrating the requirements while supplementing with other relevant compliance practices

### National security review

When network data processors engage in data processing activities that affect or may affect national security, they must undergo a national security review in accordance with relevant state regulations.

*Other references: NSL, CSL, DSL, Security Protection Regulations for Critical Information Infrastructure, Cybersecurity Review Measures, etc.*

### Personal information protection

The overall compliance requirements for personal information processors should be based on the Personal Information Protection Law and other relevant personal information protection regulations, standards and guidelines. Supplemental requirements noted from the Regulation include:

- Clearly define the conditions for transferring personal information and the specific implementation of data retention.
- Records of the data processing when providing personal information to other network data processors or entrusting them to process it should be retained for at least 3 years.
- For network data processors handling personal information of more than 10 million individuals, relevant requirements apply. These include appointing a data security officer, establishing a data security management organisation, and conducting adequate assurance and reporting when there is entity level change which might affect data security.

*Other references: PIPL, CSL, GB/T 35273 Personal Information Security Specifications, etc.*

### National security review

The overall compliance requirements for cross-border data transfer should be based on the Cybersecurity Law, Personal Information Protection Law, Data Security Law, and other related latest regulations for cross-border data transfer. Supplemental requirements noted from the Regulation include:

- The state shall take measures to prevent and address cross-border security risks and threats related to network data. No individual or organisation is allowed to provide programs, tools, or other means specifically designed to damage or bypass technical measures. Knowing that others are engaged in such activities, one must not provide them with technical support or assistance.

*Other references: CSL, PIPL, DSL, Security Assessment Measures for Cross-border Data Transfer, Measures on the Standard Contract for Cross-border Data Transfer of Personal Information, Provisions on Promoting and Regulating Cross-border Data Transfer, etc.*

# Requirements for special processing activities (cont'd) – Network platform service provider management

## Network platform service provider management

The management requirements for data security of network platform service providers are proposed for the first time in the Regulation. They mainly include:

- Clearly defining the network data security protection obligations of third-party product and service providers that access their platform, and urging these third-party providers to strengthen network data security management. In particular, network platform service providers that distribute applications must establish application verification rules and conduct network data security-related verifications.
- Allowing for personalized recommendations to be easy to turn off and personal characteristic tags to be removable for information pushed to individuals through automated decision-making processes.
- Encouraging network platform service providers to support users in using public services for national network identity authentication to register and verify real identity information.

In addition, **large network platform service providers should**:

- Publish an annual social responsibility report on personal information protection.
- When providing network data across borders, follow the requirements for cross-border data security management and improve relevant technical and management measures to prevent cross-border security risks related to network data.
- Refrain from using network data, algorithms, or platform rules to engage in improper network data processing activities that harm users' legitimate rights.
- If it involves the processing of key data, conduct an annual risk assessment that explains the security status of key business operations and the supply chain related to network data.

"**Network platform service provider**" offers services to a large number of users and operators within the platform, which may include: social media platforms that provide information publishing and interaction, online platforms that offer payment services, online platforms that provide audio-visual services, online platforms that offer application distribution services, and manufacturers of smart devices with pre-installed applications, etc.

"**Large network platform service provider**" refers to platforms with more than 50 million registered users or more than 10 million monthly active users, with complex business categories, whose network data processing activities have significant impacts on national security, economic operations, and the livelihoods of the citizens.

# Requirements for special processing activities (cont'd) – Key data management

## Key data management

The Regulation set clear requirements for processors of key data in the following areas :

**Data Security Strategy and Governance**

- ✓ A data security officer and data security management organisation should be clearly defined. The data security officer must possess professional knowledge in data security and relevant management experience, and should be a member of the network data processor's management team, with the authority to report the network data security status directly to the relevant authorities.
- ✓ In the event of mergers, divisions, dissolution, bankruptcy, or other similar situations, a report must be submitted to the relevant authorities at or above the provincial level.
- ✓ An annual risk assessment of its network data processing activities should be conducted, and the risk assessment report must be submitted to the relevant authorities at or above the provincial level.

**Data Security Lifecycle Management**

- ✓ Providing, entrusting the processing of, or jointly processing must comply with additional requirements (e.g. risk assessment, retaining records of processing activities for at least 3 years, etc.)

**Data Security Management Framework, Technology and Operation**

- ✓ The state encourages the use of data tagging and labelling tools to enhance the security management of key data.

Currently, some industry regulatory authorities have provided more clarity regarding the identification and protection of important data. They have defined the scope of important and general data in sectors such as industry, telecommunications, healthcare, and education by detailing their data classification structures. Additionally, certain free trade zones have issued detailed regulations and guidelines for identifying important data, such as the "Administrative Measures on Negative List for Outbound Data Transfer from China (Beijing) Pilot Free Trade Zone (for Trial Implementation)" and the "Standards for Data Classification and Grading by Enterprises in China (Tianjin) Pilot Free Trade Zone".

For industries where the definition and identification rules of important data are not yet well established, the "GB/T 43697-2024 Data Security Technology – Rules for Data Classification and Grading" and the "Information Security Technology – Guidelines for Identifying Important Data(Draft for Comments)" provide references that can guide the identification process.

- Industrial manufacturing
- Telecommuni-cation
- Transportation
- Financial service
- Natural Resources
- Healthcare
- Education
- Technology

### Industrial manufacturing

- Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation)
- Guidelines for Identification of Important Da ta in the Industrial Field (YD/T4981-2024)
- Several Provisions on Automotive Data Security Management (Trial)

### Financial service

- Administrative Measures of the People's Bank of China for Data Security in Business Fields (Exposure draft)
- Administrative Measures for Data Security of Banking and Insurance Institutions (Exposure draft)
- Guidelines for Data Security Classification (JR/T 0197-2020)

### Telecommunications

- Guidelines for Identification of Key Data in the Telecommunications Sector (YD/T3867-2024)

### Healthcare

- Guidelines for Data Classific ation in the Healthcare Industry (Trial)

### Education

- Guidelines for the Identification of Core Data and Key Data in the Education System (Trial)

# Recommended actions

> “Implement classified protection on network data, clearly define the responsibilities of various parties, and enforce network data security measures. It is essential to clarify security boundaries to ensure that data flows legally, orderly, and freely. This will create an environment conducive to promoting high-quality development of the digital economy and facilitating technological and industrial innovation.”

## Optimise and implement data security classification

Further promote the effective implementation of data security classification by integrating compliance requirements with internal needs. Achieve a seamless connection between data asset classification and data security levels. Utilise technology and tools for data security classification and expand its coverage on data processing activities and system applications, laying a robust foundation for data lifecycle protection.

## Establish and enhance data security governance

Promptly establish and improve the data security governance, including but not limited to data security protection principles, data lifecycle security management principles, data security incident management and emergency plans, data security complaint handling mechanisms, and data security risk and compliance management mechanisms.

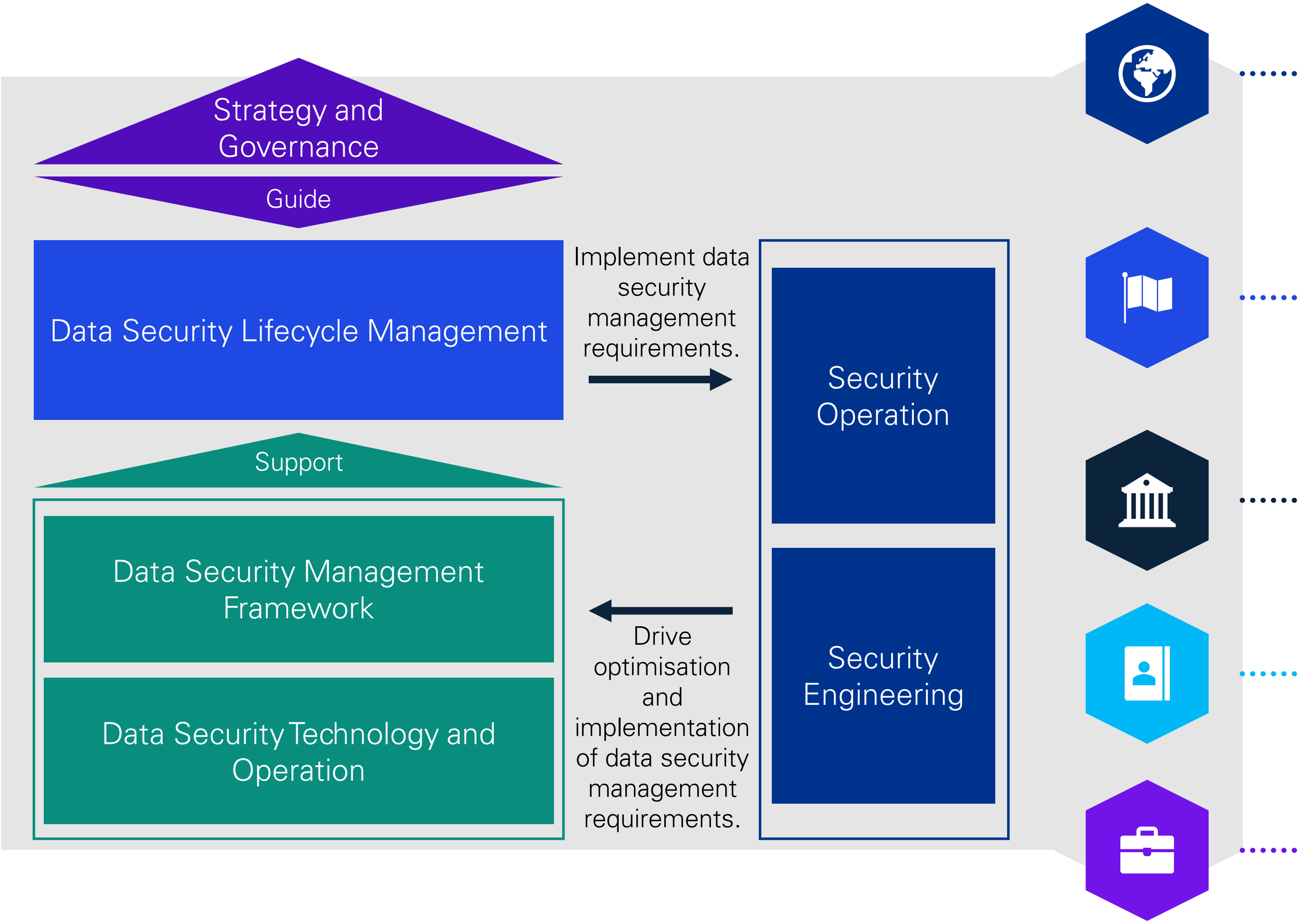
## Strengthen management framework and prioritise technical improvements

For data with higher security levels and its associated system platforms and infrastructures, prioritise implementing robust data security management measures such as enhanced encryption controls, access controls, backup/recovery processes, and log/event monitoring to effectively safeguard the integrity, confidentiality, and availability of such data.

## Consider integration with privacy and security operation activities

Personal information, as a special type of data, requires dedicated management practices. The internal data security management organisation and personnel should effectively integrate the existing personal information protection into their framework and align it with traditional information and cybersecurity measures. Consider re-evaluating and adjusting existing cybersecurity measures to ensure comprehensive data security safeguards are in place.

# KPMG provides one-stop solutions for managing data security risks



Strategy and Governance
Guide
Data Security Lifecycle Management
Implement data security management requirements.
Security Operation
Support
Data Security Management Framework
Data Security Technology and Operation
Drive optimisation and implementation of data security management requirements.
Security Engineering

### Data security classification design and implementation

Data security classification standards and tools design, data security classification management process design and implementation, and data security classification implementation, etc.

### Data security management governance planning and implementation

Data security management maturity assessment, data security management enhancement plan, data security management system design and implementation, cross-border data transfer compliance management, etc.

### Data security risk assessment / special review

Regular data security risk assessment, data security special audit for high-risk systems such as data warehouse/data lake/data management platform, etc.

### Data security incident response management

Emergency response plan, training, and drill, etc.

### Data leakage prevention management

Data leakage prevention requirement analysis, tool/vendor selection, technical implementation support and project management, etc.

# Contact Us

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

**Brian Cheung**
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +852 2847 5062
Mail: brian.cheung@kpmg.com

**Jason Li**
Director
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (10) 8508 5397
Mail: jz.li@kpmg.com

**Danny Hao**
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (10) 8508 5498
Mail: danny.hao@kpmg.com

**Lanis Lam**
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +852 2143 8803
Mail: lanis.lam@kpmg.com

**Quin Huang**
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 2355
Mail: quin.huang@kpmg.com

**Frank Wu**
Director
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 3180
Mail: fm.wu@kpmg.com

**Kevin Zhou**
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 3149
Mail: kevin.wt.zhou@kpmg.com

**Jason Song**
Director
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 2888
Mail: jason.song@kpmg.com

**kpmg.com/cn/socialmedia**

For more detail about KPMG China please scan the QR code or visit： https://home.kpmg/cn/zh/home/about/offices.html

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.