February 20, 2023

China MIIT Releases Data Security Management Measures for Industrial and Information Technology Sectors

By Liza L.S. Mark and Tianyun (Joyce) Ji

On December 13, 2022, the Ministry of Industry and Information Technology of the People's Republic of China ("**MIIT**") issued the "***Industrial and Information Technology Sector Data Security Management Measures (for Trial Implementation)***" (*《工业和信息化领域数据安全管理办法（试行）》*), which came into effect on January 1, 2023 (the "**New Measures**").

These New Measures are implementation rules under China's data security regime applicable to data processing activities in the sectors of industrial and information technology, and corresponding security supervisions. This article provides an overview of some of the important concepts in the New Measures.

1. Data Categories and Applicability

The New Measures are applicable to three types of data: (i) industrial data, which is data generated and collected by industrial businesses during R&D, manufacturing, business management, operation maintenance, platform operations, etc., (ii) telecom data, which is data generated and collected during telecom business operations, and (iii) radio data, which includes radio frequencies, stations and other radio wave parameters data generated and collected in the conduct of radio business activities. Sources of data include data from R&D, manufacturing, operation, management, services, etc.

"Data Processor" is defined in the New Measures as businesses that self-determine their data processing[1] goals and methods, which can include industrial businesses, software and IT service businesses, telecom operators and stations, etc. It is worth noting that "industrial" captures a wide range of businesses, ranging from raw materials to manufacturing sectors such as auto, mechanical, consumer goods, etc.

2. Data Classification and Management

China's data security regime classifies data into three levels: regular, important, and core. According to Articles 7 and 8 of the New Measures, the responsibility is on each Data Processor to identify and classify its data (i.e., data-mapping), and to adopt appropriate security measures for different data classifications, according to industry standards and guidelines to be further enacted by the MIIT.

Articles 9 through 11 set out respective criteria for how regular data, important data, and core data should be determined. The determining factor is upon a data breach – including tampering, sabotage, leak, or

[1] Data processing activities include but are not limited to the collection, storage, use, processing, transmission, providing, and publication of data.

misappropriation – the level of harm possible to national security, public interests, or the individual's or the organization's legitimate interests.[2]

3. Full Lifecycle Security Management

The New Measures introduce the concept of "*Full Lifecycle Security Management*" which requires Data Processors to safeguard data generated throughout its entire lifecycle, including, but not limited to, the collection, storage, use and processing, transmission, supply, and publication of the same. Specifically, according to Article 13, Data Processors are required to: (i) establish security management systems, including classification requirements and operational protocols, around the data's full lifecycle, (ii) equip data security management personnel, (iii) adopt personnel access and permissions to data, (iv) develop emergency plans and conduct emergency drills in response to data breaches, and (v) conduct regular awareness trainings. Data Processors should record and retain logs for at least 6 months relating to data processing, authorization, and access, etc.

Additional care should be used when dealing with important and/or core data. Specifically:

a. Improve Internal Management of Data. Article 13 further provides that Data Processors of important data and/or core data should: (i) establish data security working systems to identify the responsible person and department for data security, (ii) clarify key personnel and responsibilities of data processing, and require that relevant personnel execute commitment letters with clear job responsibilities, obligations, penalties, precautions, etc., and (iii) establish internal working mechanism of registrations and approvals, so as to have a sound management and record-keeping system for the handling of important data and core data.

b. Filings of Data Directory. Article 12 of the New Measures requires Data Processors to file a directory of its important and core data with the local authority. The information includes the data's sources, categories, size, processing goals and methods, scope, responsible parties, transmissions, and protection measures, but not the data itself.

c. Filings of Data Directory. Article 12 of the New Measures requires Data Processors to file a directory of its important and core data with the local authority. The information includes the data's sources, categories, size, processing goals and methods, scope, responsible parties, transmissions, and protection measures, but not the data itself.

d. Restrictions on Outbound Transmission of Data. According to Article 21 of the New Measures, for important and core data that is collected and/or generated in China, Data Processors need to have an export security assessment[3] if necessary to transfer overseas. In addition, requests (of industrial and IT sectors data, regardless of regular, important, or core) made by foreign jurisdictions will need MIIT approval prior to any transmission.

---

[2] For example, data should be considered "important data" when its breach poses threats to a wide range of "key areas" which can include politics, national lands, military, economy, culture, society, technology, natural resources, technological, electromagnetic, network, eco, resources, nuclear, as well as data that concerns China's overseas interests and key areas relating to national security such as biology, space, polar region, deep sea, and artificial intelligence.

[3] See *Measures for the Security Assessment of Outbound Data Transfers (2022)* (《数据出境安全评估办法》)

The New Measures have further clarified the responsibilities of the regulatory authorities, and we expect that detailed corresponding implementation standards and data classification categories could be expected from the MIIT soon. Businesses in the sectors of industrial, IT and software services – especially if dealing with the processing of important and/or core data – should be prepared to set up an internal management system suitable to their respective situations accordingly.

For more information, please visit our China Updates page or see the following resources:

A New Guideline Added to China's Data Protection Framework, August 17, 2022

China Revises its Anti-Monopoly Law 14 Years After its Initial Implementation, July 26, 2022

China Releases Judicial Interpretation of Anti-Unfair Competition Law, April 28, 2022

Select Proposed Changes to the Company Law of the People's Republic of China, March 22, 2022

A Snapshot of China's Cyberspace Administration and Data Protection Framework, February 9, 2022

China Intensifies Regulations on Cryptocurrency Trading and Mining, November 2, 2021

China's Amended Administrative Penalty Law Took Effect on July 15, October 8, 2021

China Issues New Rules Regulating Personal Information Collection by Mobile Apps, April 28, 2021

A New Gateway to China – Recent Policy Developments in the Hainan Free Trade Port, April 6, 2021

China Issues Measures for the Security Review of Foreign Investments, February 9, 2021

China Patent Law Fourth Amendment—Impact on Foreign Companies, January 26, 2021

China Regulators Remove Restrictions on Insurance Fund Investment, December 14, 2020

China Adopts Interim Provisions on the Review of Concentrations of Business Operators for the AntiMonopoly Law, November 30, 2020

China Releases Draft Personal Data Protection Law for Comments, November 12, 2020

China Adopts Export Control Law, November 5, 2020

China Releases New QFII/RQFII Rules, October 27, 2020

China Releases Provisions on Strengthening the Supervision of Private Equity Investment Funds (Draft), October 15, 2020

China Releases Provisions on the Unreliable Entity List, October 5, 2020

China Releases Revised Measures on Handling Complaints of Foreign-Invested Enterprises, September 23, 2020

China Releases Administrative Measures for Strategic Investment by Foreign Investors in Listed Companies, September 10, 2020

China Releases Draft Data Security Law, September 8, 2020

China Releases Circular on Further Stabilizing Foreign Trade and Foreign Investment, August 24, 2020

China Releases Draft Measures for the Administration of Imported and Exported Food Safety, August 18, 2020

U.S. Listed Chinese Companies: Regulatory Scrutiny and Strategic Options, July 30, 2020

China Passes Controversial Hong Kong National Security Law, July 9, 2020

China's Relaxed Financial Sector May Aid Foreign Investors, June 18, 2020

Is There a Law in China Similar to the US Defense Production Act?, May 8, 2020

Coronavirus Brings Force Majeure Claims to LNG Contracts, March 4, 2020

The Rise of China, March 4, 2020

Coronavirus Fears Cast Cloud Over Dealmaking, February 27, 2020

Additional questions? Please contact Haynes and Boone lawyers Liza L.S. Mark and Tianyun (Joyce) Ji.