Legal Commentary

March 10, 2022

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

A Step Forward: MIIT Again Seeks Public Comments on Administrative Measures for Data Security

Authors: Kevin DUAN | Kemeng CAI[1]

On February 10, 2022, the Ministry of Industry and Information Technology ("**MIIT**") issued a second draft of the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* (the "**Measures**"), which makes revisions to the first draft in response to public comments received following its issuance on September 30, 2021. This second draft opened for public comments until February 21, 2022.

Since 2021, the MIIT and the Cyberspace Administration of China ("**CAC**") have proposed detailed rules to implement the *Data Security Law of the People's Republic of China* (the "**Data Security Law**") and the *Personal Information Protection Law of the People's Republic of China* (the "**PIPL**"), which focus on implementation in distinct fields. To strengthen data security management in the field of industry and informatization, the MIIT has issued the Measures to implement provisions of the Data Security Law and other relevant laws and regulations. The Measures provide approaches to apply the national data security management mechanism in the field of industry and informatization in an effort to establish the data security supervision and administration system in the field of industry and informatization, through further clarification of the data classification and data grading system, management of important data and core data, and other specific requirements[2]. In respect of cyber data[3], the CAC released the *Regulations for the Administration of Cyber Data Security (Draft for Comment)* ("**Cyber Data Regulations**") for public comment on November 14, 2021. The Cyber Data Regulations propose rules for implementing relevant systems established by the Data Security Law and the PIPL; they also refine relevant requirements imposed by those laws while creating some new ones, such as the filing and annual reporting obligations of important data processors, security management duties of data processors that undertake cross-border data transfers, and responsibilities to be assumed by Internet platform operators.

---

[1] Yibing Zhao, a Han Kun intern, also contributed to this legal commentary.

[2] Please refer to the drafting notes of the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* by clicking: https: //www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf.

[3] "Cyber data" refers to any data recorded in electronic form, which is not limited to data generated by using the internet or network or processed therein. For more information, please click: https：//mp.weixin.qq.com/s/3uewzfNMEP_2Rr9SpaULnw.

Both at their formulation stage, the Measures and the Cyber Data Regulations are implementing rules respectively issued by China's two major data security regulators. Despite certain overlap between the two, they highlight different regulatory aspects due to the nature of the data they regulate, reflecting the different regulatory scopes and approaches adopted by the MIIT and the CAC.

As revised, the Measures comprise 41 articles in eight chapters (fewer than the previous 44 articles) and differ from the first draft in the following aspects:

- Separate protection for personal information: PIPL added as an enabling law.
- Expanding definition of data: includes radio data into the regulatory scope.
- Further clarifies regulators' scope of authority: confirms MIIT's supervisory role over local regulatory departments.
- Revises data classification and data grading standards: changes made to grading criteria and categorization methods.
- Clearer guidance for the filing system: more specific requirements for filing applications, filing reviews, and change filings.
- Persons responsible for data security: shifts primary responsibility to legal representatives and tightens internal management requirements for enterprises.
- Updated requirements for full life-cycle data management: removes language prohibiting core data exports and imposes security obligations for processing core data among different persons.
- Coordinates data security reviews: adds flexibility to provisions on security assessments, cooperation with supervision, and other requirements.

Below, by comparing the first draft Measures (0930) and the revised draft Measures (0210), we summarize and comment on key adjustments made in the revised draft.

Separate protection for personal information: PIPL added as an enabling law

As stressed in its drafting notes, the Measures (0930) adhere to the philosophy of the Data Security Law, which emphasizes control over personal information by categorizing it in catalogues of important data and core data, thus implementing full life-cycle security management of personal information without imposing any separate protection requirements for personal information[4]. Given that, the Measures (0930) cited as their enabling laws the Cybersecurity Law and the Data Security Law, not the Personal Information Protection Law. However, the Measures (0210) add the PIPL to the list of enabling laws and correspondingly adjust other relevant provisions with respect to personal information. For example:

[4] Please refer to the drafting notes of the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* by clicking: https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf

- "Personal information" is removed from the list of data categories in Article 8 (Methods of Data Classification and Data Grading), where non-personal information categories are retained, such as management data, operation and maintenance data, and research and development data.
- The following provision is added as Article 37 (Personal Information Protection) in Chapter 8 (Supplementary Provisions): "Data processing activities involving personal information shall also be subject to relevant laws and administrative regulations."

Given the above changes in the Measures (0210), it appears that the MIIT has turned its personal information protection approach away from "unified management by categorizing personal information in the catalogue of important data and core data" and is heading toward separate protection of personal information. This shift of direction conforms to regulatory documents issued mainly after the Measures (0930). On November 14, 2021, the Cyber Data Regulations were issued for public comments, in which personal information was not covered by the specified definitions of important data and core data. In addition, a revised public comment draft of the *Information Security Technology - Guideline for Identification of Critical Data (Draft for Comment)* (the "**Guideline**") issued by the Secretariat of the National Information Security Standardization Technical Committee on January 13, 2022, as well as its initial draft for public comment released on September 23, 2021, both define important data clearly as "not including state secrets and personal information, but may include statistical data and derived data formed on the basis of massive quantities of personal information." To achieve consistency and coordination among relevant laws and regulations, the Measures (0210) change their approach to personal information management, emphasizing the PIPL's role as the legal basis for personal information protection.

Expanded definition of data: includes radio data into the regulatory scope

The Measures (0210) revise Article 3 (Definition of Data) as follows:

- Data in the field of industry and informatization are clearly categorized into three types, namely industrial data, telecoms data, and radio data.
- Specifically enumerated industry fields are removed: Article 3 of the Measures (0930) enumerated several industries in the field of industry and informatization, such as "raw material industries, equipment industries, consumer goods industries, electronic information and manufacturing industries, software and information technology service industries, and industrial explosive materials industries". The Measures (0210) replace this enumeration with a generalized, more abstract expression, i.e., "the field of industry and informatization", to avoid legal issues that may arise in reconciling a non-exhaustive list and changes in practice.
- Adds the definition of radio data: "Radio data refers to radio frequencies, radio stations and other radio wave parameters data generated and collected in the course of radio service activities". Corresponding changes are also made in other provisions. For example, "users of radio frequencies and stations" are added as data processors in the industry and informatization field; radio regulatory authorities are recognized as data security regulators; and electromagnetic security is included as an affected area when identifying important data and core data.

Further clarifies regulators' scope of authority: confirms MIIT's supervisory role over local regulatory departments

The Measures (0210) further specify the functions and powers of data security regulators at the central and local levels:

- The central level: The MIIT's supervision and administration activities should be subject to the State's coordinated data security working mechanism. This precondition underlies the State's overall coordination over data security work at all levels and is added to cope with existing situations where data security regulation is decentralized among multiple authorities.
- The local level: the Measures (0210) call for a hierarchical supervision framework, which is absent in the Measures (0930), specifically the MIIT's responsibility to supervise and direct local departments of industry and information technology, local telecommunications administrations, and local radio regulatory authorities in all provinces, autonomous regions, municipalities directly under the central government and municipalities with independent planning status, and the Xinjiang Production and Construction Corps; also, local industry and information technology authorities, local telecommunications administrations and local radio regulatory authorities are responsible for supervising data processing activities within their jurisdictions.
- Particularly, local regulators of the industries/fields above are required to cooperate with competent authorities in carrying out data security supervision and administration activities pursuant to relevant laws and administrative regulations.

Revises data classification and data grading standards: changes made to grading criteria and categorization methods

The Measures reiterate management requirements for data classification and data grading stipulated in the Data Security Law. The Measures (0210) make revisions to the data classification and grading working requirements and methods, as well as the criteria for identifying general data, important data, and core data, mainly in the following aspects.

- Working requirements: In the Measures (0210), the provision entitled "working requirements for data classification and data grading" is set forth as Article 7; in addition to the obligations to report catalogues of important data and core data to the MIIT, local industry and information technology departments, telecommunications administrations, and radio regulatory authorities are also required to report changes and updates to those catalogues; moreover, the requirement for enterprises to "first classify data, then grade data" is removed.
- Data classification and grading methods: According to the Measures (0210), data processors in the field of industry and information technology are allowed to subdivide the categories and grades of data based on a three-tier grading system under the Measures.
- Grading criteria: the test for distinguishing general data and important data is removed, i.e., "the price range for recovery of data or elimination of negative impacts"; a radio data-related scenario is added to the criteria for identifying core data.

However, enterprises still await clearer guidance in practice for how to implement the classification and grading of important data and core data, because the Measures lack quantified standards to identify factors such as “materially affect”, “severely affect”, or “materially damage”.

Clearer guidance for the filing system: more specific requirements for filing applications, filing reviews, and change filings

Based on the Measures (0930), the Measures (0210) provide further guidance for data processors’ obligations to file catalogues of important data and core data, specifically in the following aspects.

- Filing authorities: Data processors in the field of industry and information technology are required to file their catalogues of important data and core data with the local industry and information technology authorities (industrial field), telecommunications administrations (telecoms field), or radio regulatory authorities (radio services field).
- Filing content: In the Measures (0210), the description of the filing content is more concise and it is clarified that the content to be filed does not include the relevant data *per se*.
- Time limit for review: Local industry and information technology authorities, telecommunications administrations, and radio regulatory authorities are required to complete their review of filings within 20 working days from acceptance of the filing application.
- Review decision: If the filing is approved, the local authority should issue a filing certificate to the applicant and report the same to the MIIT; where the filing is rejected, the local authority should promptly communicate the decision, along with the grounds for rejection, to the applicant.
- Change filings: If the category or quantity of important data and core data changes by more than 30%, or, if there are significant changes with respect to other particulars, the data processor is required to complete a filing for such changes within three months after they occur.
- Update filing status: In case of destruction of important data and core data, the data processor is required to update the relevant filing status with its filing authority.

Persons responsible for data security: shifts primary responsibility to legal representatives and tightens internal management requirements for enterprises

The Measures (0930) stipulated that the first step for enterprises in fulfilling their data security management obligations was to establish and improve their data security leadership system. The Measures (0930) further provided that the Party committee (group) or leadership team would undertake primary responsibility for data security, the head of the enterprise is the first responsible person for data security, and the person in charge of data security is the person directly responsible for data security. The Measures (0210) consolidate the previous Article 13 (Subject Responsibilities), Article 14 (Working Systems), Article 15 (Key Position Management), and Article 16 (Data Collection) into a sole Article 13 (Subject Responsibilities) and modify the provisions as follows.

- Legal representative as the first responsible person: The "primary responsibility for data security" taken by "the Party committee (group) or leadership team of an enterprise" under the Measures (0930) is shifted to "the legal representative or head of the enterprise", who would be "the first responsible person for data security" under the Measures (0210). The shift is sensible in that the Party committee (group) or leadership team, as an administerial organizational design, is not applicable to all enterprises, whereas a legal representative, the essential, principal role created by the Company Law, is more suitable to take primary responsibility for the data security of an enterprise.

- Stricter internal management requirements for data processors: Stricter requirements are imposed on important data and core data processors to "establish internal registration and approval mechanisms to strengthen management and keep track of important data and core data processing activities".

Therefore, we recommend enterprises that process important data and core data to pay close attention to the above changes and to adjust their organizational structures going forward. Legal representatives, first responsible persons, directly responsible persons, and key personnel who are subject to data security responsibilities should attach greater importance to data compliance and take active part in data security trainings, so as to improve their data management expertise.

Updated requirements for full life-cycle data management: removes language prohibiting core data exports and imposes security obligations for processing core data among different persons

The Measures (0210) update the general requirements for protection of various grades of data in the full life-cycle of data management, as well as the additional requirements for the processing of important data and core data. We recommend enterprises to pay attention to the following changes in the compliance requirements:

- Data storage: Data processors that store important data and core data are required to carry out data recovery tests on a regular basis.

- Data use and data processing: The Measures (0210) remove the provision that prohibits data processors from "conducting unauthorized data processing activities such as precise user profiling and data recovery targeting specific subjects by using data mining, association analysis, or other technical means".

- Data disclosure: The provision is also removed that prohibits disclosure of data "involving individual privacy, personal information, trade secrets, and confidential business information".

- Destruction of data: The Measures (0210) add a provision that requires data processors who desire to "destroy important data and core data" to "update the relevant filing status with their local industry and information technology department industrial field), telecommunications administration (telecoms field), or radio regulatory authority (radio service field)".

- Data exports: The provision is removed that prohibits cross-border transmission of core data. Instead, the Measures (0210) stipulate that, where it is truly necessary to transfer core data and important data abroad, data processors must conduct a data export security assessment in accordance with laws and regulations.

- Processing core data among different persons: The Measures (0210) add the following provision as Article 24: Where different persons are involved in the provision, transfer, or entrusted processing of core data, the data processors shall conduct data security assessments, take necessary security protection measures, and have the same reported to the MIIT through the competent local industry and information technology departments (industrial field), telecommunications administrations (telecoms field), or radio regulatory authorities (radio services field). The MIIT will review the reported activities in accordance with relevant laws and regulations.

- Responding to user complaints: Article 29 of the Measures (0930) imposed mandatory obligations on data processors to "establish user complaint response mechanisms, providing the public with easy and effective access such as e-mail addresses, telephone numbers, fax numbers and online customer services, designating personnel to accept and handle data security-related complaints from users, and giving reply within 15 working days after receiving the complaint." The Measures (0210) replace these mandatory requirements with "encourage data processors in the field of industry and information technology to establish user complaint response mechanisms", easing data processors' compliance burden in responding to user complaints.

Coordinates data security reviews: adds flexibility for security assessments, cooperation with supervision, and other requirements

According to the Measures (0930), the State will implement data security supervision and administration through data security inspection, assessment, authentication, supervision, inspection and security reviews. Enterprises are obligated to conduct security assessments, assist with regulators' supervision and inspections, and pass data security reviews. The Measures (0210) make the following changes that would add flexibility in Article 5 (Data Security Monitoring, Authentication and Assessment) and Article 6 (Supervision and Inspection):

- Relaxing regulation on authentication institutions: Article 32 of the Measures (0930) required the MIIT and local regulatory departments to establish an institutional system for data security detection, assessment and authentication by means of setting institution accreditation standards and carrying out relevant work such as selecting and accrediting institutions, granting qualifications, daily management, and issuing institution catalogues. The Measures (0210) remove the above selection and accreditation obligations imposed on regulatory departments. Instead, the Measures (0210) stipulate that "the MIIT shall encourage and guide qualified institutions to carry out data security detection and authentication pursuant to relevant standards."

- Cancelling the self-assessment provision for general data processors: Article 33 of the Measures (0930) encouraged general data processors to conduct self-assessments. The Measures (0210)

delete this provision and only require important and core data processors to conduct assessments on their own or entrust a third party to do so.

- Removing data processors' obligation to set aside an inspection interface: Under Article 34 of the Measures (0930), enterprises were obligated to cooperate with industry regulators in their supervision and inspections and to set aside an inspection interface for use. Accordingly, the major issues of concern for enterprises would have been the scope of inspection, technical standards of the inspection interface, and interface access conditions. However, the Measures (0210) remove this obligation to set aside an inspection interface and enterprises are only generally required to cooperate with regulators' inspections.

- The Measures (0930) provided at Article 35 that the MIIT will, under the coordinated working mechanism for national data security review, conduct data security reviews of processing of industrial and telecoms data that affect or may affect national security. On the other hand, on January 4, 2022, 13 ministries and commissions, including the Cyberspace Administration of China and the China Securities Regulatory Commission, jointly promulgated the revised *Measures for Cybersecurity Review*, which subject data processing activities into the scope of review, stipulating that key factors for assessment include "the risk for core data, important data or large quantities of personal information to be stolen, leaked or destroyed, or illegally used or taken abroad." Therefore, under the Measures (0930), data processors would have faced two reviews pursuant to the MIIT's administrative measures and the CAC's *Measures for Cybersecurity Review*, respectively. However, under the Measures (0210), the MIIT is only required to carry out data security review work under the coordinated working mechanism for national data security review and is no longer obligated to "conduct data security reviews of industrial and telecoms data processing that affect or may affect national security." This change leaves flexibility for the MIIT and the CAC in their coordination of data security reviews.

Conclusion

Compared to the first draft, the Measures (0210) make quite a number of changes. In addition to the substantial compliance obligations mentioned above, the revised draft also makes changes in terms of wording and the assumption of legal liability (e.g., It removes the provision that incorporates data processors' data security liability into the credit management system and puts those who commit data security violations on the blacklist of dishonest subjects). The second draft coordinates the Measures with relevant laws and regulations, rectifies the wording of relevant concepts, and adds flexibility to supervision and compliance approaches. As the overarching regulatory design in the field of industry and information technology, the Measures set forth many specific compliance requirements to which enterprises in the industry and information technology field should pay great attention.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com

Kemeng CAI

Tel: +86 10 8516 4289
Email: kemeng.cai@hankunlaw.com