Establishing Framework for Data Compliance in Industry and Information Technology Sectors (Part I)

作者：
傅鹏 Fu, Peng (Victor)
赵卿梦 Zhao, Qingmeng
钱学悦 Qian, Xueyue

After the three cornerstone laws in the area of data compliance (i.e., the Cybersecurity Law of the PRC ("**CSL**"), the Data Security Law of the PRC ("**DSL**"), and the Personal Information Protection Law of the PRC ("**PIPL**")) were issued, the governmental authorities begin formulating implementation rules to establish the data compliance frameworks for specific industry sectors or regulatory areas.

Rules have been issued for some heavily regulated sectors, such as the financial sector, the healthcare sector, and the automotive sector. However, a large amount of entities do not fall into the categories of these sectors. Among others, the industry and information technology sectors cover numerous enterprises. The entities in such sectors process huge amounts of data in their daily operations, and their data processing activities play a vital role in safeguarding the daily operations of many sectors and protecting the economic development security of the country. The governmental authorities and the market expect to see when and how the data processing activities in such sectors would be regulated.

On December 13, 2022, the Ministry of Industry and Information Technology of the PRC ("**MIIT**") issued the Administrative Measures on Data Security in the Industry and Information Technology Sectors (for Trial Implementation) ("**Measures**"). The Measures establish the framework of data compliance in the industry and information technology sectors, which include the following important topics: (1) what businesses and what entities in such sectors are subject to the regulation of the Measures, (2) how are the data processors in these sectors required to categorize and classify their data and how should the catalog of important data and core data be filed with competent governmental authorities; (3) how should data processors in such sectors protect and manage their data throughout the data life cycle; and (4) how should governmental authorities and data processors establish mechanisms for monitoring data security risks and how should data processors report data security incidents.

In this article, we present Part I of our comments on the Measures and our analysis about how would the Measures be applied and implemented in practice. Our comments and analysis in this article include what businesses and what entities are subject to the Measures, how are the data processors required to categorize and classify their data, and how should the catalog of important data and core data be filed with competent governmental authorities. In our next article (Part II of our comments and analysis), it will include how should data processors in such sectors protect and manage their data throughout the data life cycle, and how should governmental authorities and data processors establish mechanisms for monitoring data security risks and how should data processors report data security incidents.

1. A regulatory scope that may have widespread regulatory effects

What sectors and entities are the Measures regulating?

The Measures regulate the processing of data in the industry and information technology sectors within the territory of the PRC.

The data in the industry and information technology sectors mean (1) industry data, i.e., data generated and collected in the process of R&D and design, manufacturing, operation and management, operation and maintenance, platform operation, etc. in various fields of industry fields and sectors, (2) telecommunication data, i.e., the data generated and collected in the telecommunications business operation activities, and (3) radio data, i.e., the radio waves parameter data generated and collected in the process of carrying out radio operations, including radio frequencies and stations.

Therefore, the Measures intend to regulate the processors which process the data in the industry and information technology sectors and which can decide the purpose and method of such processing activities ("**Processor**"). The Processors include industrial enterprises, software and information technology services enterprises, telecom service providers which have obtained telecom business licenses, and entities that use radio frequencies or radio stations, and other entities in the industry and information technology sectors. The activity of processing data includes data collection, storage, use, processing, transmission, provision, disclosure, etc.

Such a regulatory approach would include a wide range of entities in its regulatory scope, especially those entities conducting typical "to B" businesses that previously have not faced such heavy pressure in the area of data compliance.

Enterprises in all sectors need to comply with data compliance requirements, especially those obligations under the three cornerstone data compliance basic laws (i.e., the CSL, DSL, and PIPL). Before the promulgation of the Measures, while the DSL mainly aims at setting up a general regulatory framework without many details, the PIPL provides a series of specific compliance requirements. This is why more companies have to put their compliance resources first in the area of complying with PIPL and relevant rules in the area of personal information protection. For compliance in this area, those enterprises conducting typical "to C" businesses (i.e., businesses that face or have individual customers directly) have more burdensome obligations, while those enterprises having typical "to B" businesses (i.e., businesses that customarily face institutional clients) may feel comparatively easier to handle compliance requirements because the number of personal information processing scenarios they handled is relatively limited and the amount of personal information they processed may be comparatively low.

This may significantly change after the Measures are issued. The requirements under the Measures cover personal information protection, but more of them focus on data that are not personal information. To be compliant with such requirements, typical "to B" enterprises (such as a large amount of enterprises in the industry and information technology sectors) need to pay more attention and devote much more resources.

Specifically speaking, the following types of enterprises may need to pay attention to the requirements under the Measures:

- Industrial enterprises

According to the Industrial Classification for National Economic Activities, mining, manufacturing, production and supply of electricity, gas and water, etc., shall be identified as industrial areas. Therefore, enterprises in such areas can be considered as industrial enterprises and may probably need to comply with the Measures.

The number of such industrial enterprises is large, and such enterprises cover a wide range of areas and businesses. Enterprises in some of such areas (such as mining, traditional manufacturing) typically process very limited amount of personal information, but they process significant amount of industrial data. The processing of such data currently needs to comply with various new requirements under the Measures.

- Software and information technology services enterprises

This type of enterprise would include a large number of software companies, internet companies, SaaS and other online service companies, big data and AI service companies and companies in the semi-conductor industry.

It is worth noting that the term "software and information technology services" undoubtedly covers numerous "to C" internet companies. Such companies directly provide services to end users through websites, mobile applications ("**APP**") or mini programs under large platforms (such as WeChat mini programs). Previously, such companies may have mainly paid attention to personal information protection requirements under the PIPL and other implementing rules. Still, from the promulgation of the Measures, such companies should also invest significant resources in complying with the Measures and submit filing materials according to various filing mechanisms established by the Measures.

- Telecom service providers which obtain telecom business licenses

Telecommunication service is a traditional area under the regulation of MIIT, but previously more focus is put in the fields of telecommunication service qualifications, i.e., a company which conducts telecommunication business needs to obtain a telecommunication business license before it conducts related business in the PRC.

The issuance of the Measures shows that MIIT will also focus on the data processing activities of such companies that operate telecommunication businesses, especially those data processing activities that do not involve personal information are now expressly included in the regulatory scope.

One thing to note is that the Measures use the wording of "telecom service providers which have obtained telecom business licenses." This means that it clearly aims to regulate those entities that provide telecom business services and that obtained or should have obtained telecom business licenses. Many companies that operate an official website for self-introduction purpose or for the promotion of the companies' products/services need to complete an ICP record filing procedure so as to register their domain name and website in MIIT's database, but such an ICP record filing is not a telecom business license. Therefore, technically speaking, a company that completes ICP record filing will not necessarily be required to comply with the Measures.

What is the regulated "territory" under the Measures?

The Measures provide that it regulates data processing activities that occur within the territory of the PRC.

To be aligned with the regulatory approach under CSL, DSL and PIPL and to be consistent with the interpretation of the term "territory" under the Exit and Entry Administration Law of the PRC, the term "within the territory of the PRC" shall mean mainland China and would not include Hong Kong, Macau and Taiwan.

It is not quite clear whether the Measures intend to have the effect of regulating certain entities outside the territory of the PRC. For example, as reflected in the PIPL and the Regulations on the Administration of Network Data Security (Draft for Comments), such laws and regulations not only regulate entities and individuals in the territory of the PRC, but also regulate those data processors which are located outside the territory of the PRC and (1) have the purpose of providing products or services to entities or individuals in the PRC, or (2) analyze or evaluate the behavior of entities or individuals in the PRC. The wording of the Measures does not contain such effect of regulating offshore entities, but entities would also wait to see whether, in practice, MIIT would have a broadened interpretation to expand the Measures' effects to such scope.

2. To formally establish the data categorization and classification system in the

industry and information technology sectors

What a Processor needs to do about the important data and core data, and what are the requirements for such a Processor to file the important data and core data catalog for record?

- Preparation of a catalog of important data or core data

A Processor should regularly review and manage its data, and should, based on relevant standards and guidelines, identify its important data and core data and establish a catalog to reflect the important data and core data (if any) of the Processor.

- To submit record filing for the catalog of important data or core data

A Processor should file its catalog of important data and core data to the relevant regulators for the industry and information technology sectors ("**Regulators**") for record. The record filing should include the following information:

- The sources, categories, levels, size, storage or processing media/carriers of the relevant important data or core data;

- The processing purposes and methods, the scope of use, the entities which bear responsibilities related to such important data or core data;

- How the Processor conducts external sharing or cross-border transfer for its important data or core data;

- What security protection measures are taken; and

- Other information that may be required.

It is worth noting that the Measures specifically emphasize that the Processor does not need to submit the data itself. This may help mitigate the concerns of the Processors who are designing their filing strategy. Also, this may help reduce the workload for such record filing preparation and may facilitate more Processors to complete the record filing in a timely way.

The Regulators should complete the review for the filed materials within twenty business days after a Processor submits its record filing materials, and decide whether or not to accept such record filing. If a Regulator decides not to accept the filing, it should inform the Processor of the reasons for such rejection, and the Processor should re-submit an improved filing within fifteen business days after it receives the rejection decision.

- To complete filing updates when filing contents changed

If there are significant changes in the record filing contents, the Processor should complete a filing update procedure within three months after the occurrence of such significant changes.

The "significant changes" mean the size of a certain type of important data or core data has changed by more than 30% (the number of data entries or the total amount of storage, etc.), or other changes in the content of the record filing.

However, such a filing update procedure seems to be still ambiguous about when it will be triggered. Among other things, the last sentence of the provision (Article 12) in the Measures provides that when other filing contents changed, a filing update procedure should be triggered. This provision can be interpreted broadly. Some typical scenarios may be that, when the name, legal representative, or other basic corporate information of the Processor changes, the Processor needs to update the record filing. It is uncertain whether any change of information indicated in the filing form will trigger the update procedure. In practice, the Regulator may probably have more detailed guidance on this.

- Open questions and the relationship between this record filing mechanism and other data-related filing systems

Also, questions may be raised regarding whether there is a fixed filing deadline, whether such filing needs to be conducted each year like what has been done by the automotive data processors, what are the specific requirements for filing and format of the filed materials, and what level of details should be included in the filing materials. These questions may probably be answered in detailed implementation guidelines to be issued by the Regulators.

Additionally, Processors may have questions about the relationship between this record filing mechanism and other established data record filing systems.

For example, as established in the Several Provisions on Automotive Data Security Management (for Trial Implementation) ("**Automotive Data Provisions**"), automotive data processors which process important data should submit a filing related to its security management of automotive data with the local branch of the Cybersecurity Administration of China ("**CAC**") and other applicable authority (which is also the local branch of MIIT, the same as the Regulator) before the date of December 15 each year.

There will be an obvious overlap between the scope of Processors and the scope of automotive data processors. Also, the key regulatory issues in the important data/core data filing mechanism are substantially similar to those issues in the automotive data processing filing system.

The Regulators may need to further address this and answer what is the relationship between the important data/core data filing mechanism and the automotive data processing filing system, and it may be a reasonable expectation to foresee that the Regulators would try to design rules to avoid a "repetitive filing" for some entities that happen to be obligated to do both filings.

How will the data in the industry and information technology sectors be categorized?

The data categories in the industry and information technology sectors may, depending on the specific industry requirements, characters, business needs, data sources and purposes of use, etc., include but not limited to the following categories:

- R&D data;
- Manufacturing and operation data;
- Management data;
- Operation and maintenance data;
- Business and services data.

It is worth noting that the categorization of data shall also take into consideration of the standards and guidelines for specific industries and businesses. For example, in the automotive industry, the Specification of Internet of Vehicle Information Service – User Personal Information Protection provides data categorization guidelines. Therefore, the categorization of data in the automotive industry shall consider such guidelines, and the final categorization results may be significantly different from the abovementioned examples.

How will the data in the industry and information technology sectors be classified, and what are the ordinary data, important data and core data?

- General classification methods and more detailed sub-classes

Data in the industry and information technology sectors shall be classified according to the degree of harm caused by such data being tampered with, destroyed, leaked or illegally obtained or illegally used, to national security, public interests or the legitimate rights and interests of individuals and entities. The most general classification approach would divide data into three classes: ordinary data, important data, and core data.

Processors could define further detailed sub-classes based on such general classification methods. In practice, various Processors may adopt different sub-classes. For example, many Processors would tend to refer to the Cybersecurity Standards Practice Guidance – Guidelines for Network Data Categorization and Classification to further sub-classify ordinary data into different levels. Processors may also sub-classify important data into different levels, with the final classification results showing six or seven classes of data.

- Identification of ordinary data

If the degree of harm, which is caused by certain data being tampered with, destroyed, leaked or illegally obtained or illegally used, fits with the following level, then such data can be identified and classified as ordinary data:

- A relatively low impact on the legitimate rights and interests of individuals and organizations, and a low negative impact on society;

- A relatively small number of affected users and enterprises in a relatively small scope of production and living areas, has a relatively short-term effect and a relatively low impact on the operation of enterprises, industry development, technological advancement, and industrial ecology;

- Other data not included in the catalogs of important data or core data.

- Identification of important data

If the degree of harm, which is caused by certain data being tampered with, destroyed, leaked or illegally obtained or illegally used, fits with the following level, then such data can be identified and classified as important data:

- A threat to the politics, territory, military, economy, culture, society, science and technology, electromagnetic, network, ecology, resources and nuclear security, and an impact on the PRC's overseas interests, biology, space, polar, deep sea, artificial intelligence and other key areas related to national security;

- A serious impact on the development, production, operation and economic interests in the industry and information technology sectors;

- Causing major data security incidents or production safety accidents, and having a serious impact on public interests or the legitimate rights and interests of individuals and organizations, with a great negative impact on society;

- Triggering obvious cascade effect, and the scope of impact involves multiple industries, regions or multiple enterprises in the industry, or the impact lasts for a long time, causing serious impact on industry development, technological progress and industrial ecology, etc.

- Other important data determined through the assessment of the MIIT.

- Identification of core data

If the degree of harm, which is caused by certain data being tampered with, destroyed, leaked or illegally obtained or illegally used, fits with the following level, then such data can be identified and classified as core data:

- A serious threat to the politics, territory, military, economy, culture, society, science and technology, electromagnetic, network, ecology, resources and nuclear security, and a significant impact on China's overseas interests, biology, space, polar, deep sea, artificial intelligence and other key areas related to national security;

- A significant impact on industry and information technology sectors and its key enterprises, critical information infrastructure, important resources, etc.;

- Significant damage to the industrial production and operation, telecommunications networks and internet operation services, radio business development, etc., which results in widespread shutdown, large-scale radio service interruptions, large-scale network and service paralysis, loss of a large number of business processing capabilities, etc.;

- Other core data determined through the assessment of the MIIT.

- Elements to consider when conducting the data identification

The abovementioned principles and definitions are provided by the Measures to describe the nature or general scope of ordinary data, important data and core data. A Processor may consider the following elements or trends to specifically guide its implementation practice:

- Area-based detailed requirements or guidelines

  In a specific business area, there may probably be more detailed guidance regarding the identification of important data or even core data.

  For example, in the automotive area, the Automotive Data Provisions expressly provide that operation data of the automobile charging network is important data, which indicates more importance of such data in the process of classification. Also, for those online healthcare service providers or those online finance-related services providers who may hold value-added telecom business licenses, they would thus be subject to the regulations of the Measure to complete data classification, and they may need to refer to the guidelines of specific areas (such as the Information Security Technology—Guide for Health Data Security in the healthcare area or the Financial Data Security – Guidelines for Data Security Classification in the finance area) to guide the specific data classification practice.

- Whether the data merely covers or is only relevant to daily business

  If certain data merely covers or is only relevant to the daily business of a commercial entity, such data may have less importance in the process of classification. For example, if certain data only includes general commercial arrangements or financial information, such data may be comparatively less important. If certain data also involves technological information or more sensitive information about the country or an industry, such data may be comparatively more important.

- The amount of sectors, territorial areas, entities or persons involved

  If certain data or data set reflects the information of more sectors, entities or persons, such data or data set may probably be more important in the classification process.

  Putting together the Measures' definitions of ordinary data, important data and core data, one important element the Measures consider is the "amount" element. If more sectors, territorial areas, entities or persons are involved in a data or data set, the compromise of such data or data set may probably cause more severe harm to the industry security, industry operation, or even national security.

  Such an approach is similar to the approach adopted in other data regulation areas. For example, when regulating cross-border data transfer, the regulators also think that if the transmission of personal information involve more than certain persons (i.e., the processor handles personal information of more than 1 million persons, or the cumulative amount of personal information provided overseas reached 100,000 persons since January 1st of the last year, or the cumulative amount of sensitive personal information provided overseas reached 10,000 persons since January 1st of the last year), then the transmission is of great regulatory significance and should be subject to CAC's review.

- The level of confidential information or non-public information involved

  If most part of a data set involves confidential information or non-public information, such data set would be more sensitive and be more important in the classification process. By contrast, if a data set only contains publicly available information, its level of sensitivity and importance might be lower.

- The level of personal information involved

Even from the perspective of data governance and data classification, the amount of personal information involved is an important element in evaluating its classification level. If a data set involves less personal information, or involves information that has been anonymized, a Processor may have more reasons, at least to some extent, to think that such a data set is comparatively less sensitive and important.

- The level of information granularity

  If a data set contains a more fine-grained description or contains more details, then its sensitivity and importance might be higher. If a data set contains a more coarse-grained description or contains less details, then its sensitivity and importance might be lower. The typical example is that, with the assumption that the same amount of data or persons are involved, aggregated data or overall descriptive results may seem to be safer and less sensitive.