LINKS Law Offices
通力律师事务所

Data-Driven Strategies and Data Compliance: A Brief Analysis of the Guidelines for Data Classification and Grading of Financial Information Services

By Sandra Lu | Lily Luo | Neil Zhao

In recent years, with the rapid development of AI, machine learning and big data, the competitive edge in global capital markets increasingly relies on data acquisition and computing capabilities. For quantitative hedge funds, proprietary trading firms and asset managers employing tech-driven strategies, massive and multi-dimensional market and industry data have become the core resources for generating trading signals and extracting alpha. For foreign institutions, whether investing directly in the Chinese market via channels like QFI or Stock Connect, or indirectly through financial derivatives such as TRS, obtaining comprehensive, accurate and continuous Chinese market and industry data is crucial for the execution of their investment and trading strategies.

Driven by the continuous growth in domestic and cross-border data demand, a group of professional financial information service providers (such as Wind, Hithink RoyalFlush, East Money, etc.) has emerged and matured in China. There are also foreign institutions approved to provide financial information services within China (such as Bloomberg, Dow Jones, etc.) (collectively "**data vendors**"). These data vendors extensively collect, process and provide multi-dimensional financial information services to domestic and foreign market participants, covering financial market data (equities, commodities, futures, indices), macroeconomic data (trade, investment, fiscal), informational report data (industry news, research reports, policies and regulations), and industry indicator data (food and beverage, transportation, tourism and hospitality). While data empowers financial innovation, the regulation and management of data security and cross-border data transfers are also being increasingly strengthened. In the field of financial information services, the regulatory logic has expanded from the approval and filing management of "financial information service providers" to the direct management of "financial information service data" itself.

On 13 June 2026, the Cyberspace Administration of China ("**CAC**"), the People's Bank of China, the National Financial Regulatory Administration, the China Securities Regulatory Commission, the National Bureau of Statistics and the State Administration of Foreign Exchange jointly issued the *Guidelines for Data Classification and Grading of Financial Information Services* ("**Guidelines**"), aiming to standardize financial information data processing activities and elevate the security level of financial information service data. For asset managers, quantitative hedge funds and proprietary trading firms that highly depend on data inputs to operate their strategies, the Guidelines are by no means merely a compliance requirement for data vendors. Once data vendors implement the classification and grading standards, substantial changes may occur in the granularity of their data collection, the desensitization methods applied to sensitive data, the scope of data services they can provide, and the processes for cross-border data transfers, thereby bringing potential impacts to quantitative models or data-driven strategies that rely on specific data sources.

I. Scope of Application of the Guidelines

The Guidelines apply to financial information service providers operating within China when conducting data classification, grading, and important data identification. According to the *Provisions on the Administration of Financial Information Services*, "financial information services" refers to the provision of information and/or financial data that may affect financial markets to users engaged in financial analysis, financial transactions, financial decision-making, or other financial activities.

According to the Guidelines, "financial information service providers" refers to legal persons and unincorporated organizations engaged in providing financial information services, excluding state organs and organizations authorized by laws and regulations to perform public affairs management functions. Meanwhile, in conjunction with relevant rules such as the *Notice on Conducting the Filing of Domestic Financial Information Services* and the *Provisions on the Administration of the Provision of Financial Information Services in China by Foreign Institutions*, as well as the relevant approval and filing lists published by the CAC, the Guidelines should primarily apply to financial information service providers that offer financial news, financial data, and market quotes to financial market participants such as professional institutions or investors. Currently, the lists of financial information service providers published by the CAC mainly include domestic financial information service providers, foreign-invested enterprises established in China by foreign institutions to provide financial information services, and foreign institutions providing financial information services in China[1]. Relevant institutions should pay close attention to the Guidelines.

II. Core Content of the Guidelines

The *Data Security Law of the People's Republic of China* established a data classification and grading protection system at the legal level, and the *Regulation on Network Data Security Management* further requires that all regions and authorities determine specific catalogs of important data for their respective regions, authorities, and relevant industries/sectors in accordance with this system. The Guidelines serve as the specific implementation of these principled requirements within the niche sector of financial information services.

---

[1] The first batch of filed domestic financial information service providers: https://www.cac.gov.cn/2022-01/04/c_1642894644935908.htm
The second batch of filed domestic financial information service providers: https://www.cac.gov.cn/2022-10/28/c_1668509064248761.htm
The third batch of filed domestic financial information service providers: https://www.cac.gov.cn/2023-11/21/c_1702230143102599.htm
The fourth batch of filed domestic financial information service providers: https://www.cac.gov.cn/2026-02/14/c_1772800146857074.htm
The list of approved foreign institutions providing financial information services in China: https://www.cac.gov.cn/2026-04/30/c_1779276540918311.htm
The list of approved enterprises established by foreign institutions to provide financial information services in China: https://www.cac.gov.cn/2026-04/30/c_1779276540092438.htm

1. Data Classification and Grading

Regarding data classification, the Guidelines adopt the approach of "first classifying by industry sector, then by business attribute" as established in the national standard *Data security technology – Rules for data classification and grading*. In the financial information service sector, data is classified according to its business attributes. The level-1 classification consists of 3 categories: business data, user data, and enterprise data. Based on this, it is further subdivided into 9 level-2 categories and 67 level-3 categories, achieving comprehensive coverage and granular management of data across different financial information service scenarios.

- Business data: Includes financial market data reflecting market dynamics and asset conditions, macroeconomic data reflecting national or regional economic performance, organizational data of financial market participants, industry indicator data reflecting sector operational status and market supply/demand, as well as informational report data such as news, commentary, and insights related to financial markets.

- User data: Divided into individual user data and institutional user data. Individual user data is further divided into basic information, transaction data, and biometric identification information. Institutional user data is further divided into basic information and transaction data.

- Enterprise data: Refers to the data of the financial information service providers themselves, divided into operational management data and system operation and maintenance data.

However, from the perspective of the actual needs of cutting-edge industry trading, the Guidelines do not yet cover certain emerging alternative data types, such as consumer transaction data, consumption habits, web scraping data, web browsing traffic, browsing habits, satellite imagery, geolocation, social media, market sentiment, public opinion data, supply chain, customs, and shipping data. This may not fully resolve the issues faced by professional institutions like quantitative hedge funds and proprietary trading firms regarding alternative data procurement and cross-border transfers.

Regarding data grading, referring to the national standard *Data security technology – Rules for data classification and grading*, the Guidelines grade data into four levels from highest to lowest (i.e., core data, important data, sensitive general data, and non-sensitive general data) based on the data's importance and sensitivity in economic and social development,

as well as the degree of harm that would be caused to national security, economic operations, social order, public interests, organizational rights and interests, or individual rights and interests if the data is leaked, tampered with, destroyed, or illegally acquired, used, or shared.

Notably, combining the specificities of the financial information service sector and the sensitivity of the data held, the Guidelines subdivide "general data" into "sensitive general data" and "non-sensitive general data" under the national data classification and grading framework. The main criteria for this subdivision are whether the data is public, whether it involves domestic or overseas situations, and the degree of impact if leaked, tampered with, or destroyed. For example, according to Appendix A of the Guidelines:

- Using "public status" as the criterion: Among fund data, undisclosed private fund data is sensitive general data, while others are non-sensitive general data; among research reports, those publicly released by licensed financial institutions are non-sensitive general data, while others are sensitive general data.

- Using "domestic/overseas" as the criterion: For macroeconomic data (e.g., national accounts, price indices, trade, investment, finance, fiscal affairs) and various industry indicator data, domestic data is in principle sensitive general data, while overseas data is non-sensitive general data.

2. Important Data Identification

According to Article 5.5 of the Guidelines, the data level should be comprehensively determined based on the identification of grading elements and the analysis of the affected subjects and the degree of impact. Summarizing the data level determination criteria provided in the Guidelines:

- Any data that causes any degree of harm to national security constitutes, in principle, important data or even core data.

- Data causing "severe harm" to economic operations, social order, or public interests constitutes important data; data causing "general harm" constitutes sensitive general data.

- Data only affecting organizational or individual rights and interests is, in principle, sensitive general data or non-sensitive general data.

Furthermore, the Guidelines establish a principle of "adopting the highest and strictest standard", meaning the level of a dataset is determined by the highest level of the data items it contains. The Guidelines also clarify that any data identified, notified, or publicly released as core data or important data by relevant authorities or regions according to their standards shall be classified and graded accordingly.

Based on the examples provided in Appendix A of the Guidelines, scenarios in the financial information service sector that may fall into the important data category mainly include:

- High-granularity domestic industry and commodity data: Domestic industry indicator data (e.g., energy, steel, non-ferrous metals, automotive, biomedicine) and commodity data are in principle sensitive general data. However, if their coverage, time span, or precision is higher than the level publicly released by relevant governmental departments (including historically released data) and can reflect situations at the provincial administrative region level or above, they are upgraded to important data. This means that domestic macro and industry data that is more precise, detailed, and broader in coverage than official data is a key target for important data identification.

- Datasets of users[2] reaching a certain scale: For example, basic information datasets of 10 million+ individual users, transaction datasets of 1 million+ individual users, biometric datasets of 100,000+ individuals, basic information datasets of 1 million+ institutional users, or transaction datasets of 100,000+ institutional users all constitute important data.

- Institutional transaction data that may directly impact national security: Institutional user transaction data that, if leaked or tampered with, could directly affect national security belongs to important data.

According to Article 5.6 of the Guidelines, data levels are not static. When data content, timeliness, scale, usage scenarios, or processing methods change, or when data fusion or requirements from national/relevant authorities render the original level inapplicable, it should be updated promptly. This means a data vendor's processing methods (e.g., increasing granularity, extending historical spans, multi-source fusion) can inherently change the data level and trigger an important data designation.

[2] In this context, "users" should specifically refer to those who procure financial information services, rather than broadly referring to general consumers or clients across various industries.

III. Impact of the Guidelines on Data Vendors

Relevant data vendors should conduct data classification and grading in accordance with the Guidelines and adopt differentiated protection measures for different categories and levels of data to fulfill their compliance obligations as data processors. The Guidelines outline a relatively complete step-by-step process: data resource mapping, data classification, data grading, forming a classification and grading catalog, reporting the important data catalog, and dynamic update management.

1. Comprehensively Mapping Data Resources and Establishing Catalogs

Data vendors should first comprehensively map their data resources, clarifying basic information, descriptive objects, and business attributes of database tables, data items, and files. Based on this, they should map data down to level-2 and level-3 categories, comprehensively determine the data level through analysis of grading elements, and ultimately form a data classification and grading catalog and an important data catalog.

2. Fulfilling the Obligation to Report Important Data Catalog

For identified important data, data vendors should report the catalog to competent authorities in the required frequency and format. According to Appendix B of the Guidelines, the reporting content is highly detailed, covering basic data information (name, classification and grading basis, level, carrier, source, volume, total storage, coverage type/ratio), responsible entity details (name of data processor, institution code, location, person in charge of data security), and data security status (IT system name, cybersecurity MLPS status, whether it is critical information infrastructure, whether data security risk assessment is conducted and risk assessment conclusions). Moreover, if the number of important data items or total storage volume changes by more than 30%, the important data catalog shall be resubmitted in a timely manner.

3. Differentiated Protection and Cross-Border Data Compliance

The significance of classification and grading lies in implementing differentiated security protection and cross-border management. Once data is identified as important data, it triggers stricter compliance requirements in accordance with the law, such as statutory cross-border data security assessment. For “sensitive general data”, though there is no statutory security assessment for cross-border transfers, its “sensitive” nature means data vendors will still exercise caution when providing it externally (especially offshore). This may cause data vendors to adjust data collection granularity, desensitization methods, the scope of available data, and cross-border transfer arrangements.

4. Potential Impact on Data Processing and Product Strategies

Notably, the Guidelines use "coverage, time span, and precision higher than officially released levels and reflecting provincial levels or above" as a key criterion for upgrading domestic industry/commodity data to important data. This actually constrains the core competitiveness of data vendors: the more they use deep processing and multi-source fusion to provide domestic data that is more comprehensive, granular, and precise than official sources, the more likely they are to cross the important data red line. Therefore, data vendors must carefully balance enhancing data value against controlling compliance levels in their product design, managing risks through grading labels, desensitization, and controlling granularity/coverage.

IV. Key Takeaways for Data Buyers

1. Cooperation and Onboarding: Verifying Vendor Compliance

For data buyers like quantitative hedge funds and proprietary trading firms, the primary focus is whether the counterparty (i.e., the data vendor) has implemented classification and grading as required under the Guidelines, and whether the compliance attributes of the provided data are clear. The requirements set out in the Guidelines should be integrated into the full lifecycle of due diligence, onboarding, and contracting:

- Due diligence and compliance verification: Conduct compliance due diligence on data vendors prior to onboarding. Key focus areas should include verifying whether the vendor has implemented a data classification and grading framework in accordance with the Guidelines, whether they maintain a comprehensive data asset inventory, and assessing their data security management capabilities alongside their historical compliance track record.

- Data scope and grading disclosure: Require data vendors to clearly define and disclose the categories and grades of the data provided (particularly whether it involves "sensitive general data" or higher-grade data), ensuring the presence of clear and identifiable data classification and grading labels.

- Contractual safeguards: Clearly stipulate data compliance representations and warranties in the service agreement, requiring data vendors to warrant the lawful sourcing of the provided data and the accuracy of its classification and grading.

- Allocation of cross-border transfer compliance responsibilities: For scenarios involving outbound data transfers, clearly define the compliance obligations of both parties and the responsibilities of the filing/reporting entity regarding cross-border data transfers within the service or security agreement.

- Dynamic adjustment and notification mechanism: Establish a routine communication mechanism stipulating that if the data vendor's classification and grading results change (e.g., non-sensitive general data is upgraded to sensitive general data), or if regulatory shifts impact the scope of data provision, the vendor must promptly fulfill its notification obligations and initiate a dynamic adjustment process for the service arrangement.

2. Data Scope: Boundaries of Procurable Data May Change

The clarification of data classification and grading rules will directly impact the scope of data that vendors can provide.

Regarding scenarios where foreign institutions procure data directly from Chinese data vendors, domestic vendors have historically adopted a cautious and strict approach in practice due to uncertainties surrounding the identification of "important data" and cross-border data transfer regulations. Consequently, the scope of data directly available to foreign institutions has been relatively narrow, sometimes failing to meet the demands of offshore trading strategies for data breadth and granularity.

Following the issuance of the Guidelines, as classification and grading standards become clearer, there is room for expansion in the scope of data available for procurement by foreign institutions. For instance, regarding "sensitive general data" that explicitly falls outside the scope of "important data", since it does not trigger prerequisite procedures such as statutory security assessment, it is theoretically feasible to transfer such data offshore. Once the regulatory boundaries are clearly defined, data vendors may moderately open up the supply of this type of data.

However, it should be noted that, though "sensitive general data" does not require a security assessment procedure, its "sensitive" nature means that data vendors may still harbor concerns about providing it directly to foreign institutions from a data security management and risk control perspective. Particularly during the cross-border transfer phase, vendors may be reluctant to shoulder the corresponding compliance burden due to difficulties in gauging the appropriate regulatory thresholds. Consequently, the practical availability of "sensitive general data" may still be constrained by the risk appetite of the individual data vendors.

3. Structural Arrangements: The Value and Challenges of Establishing an Onshore Entity

Given the potential supply constraints that "sensitive general data" may face during cross-border transfers, establishing an onshore entity for transition and processing may serve as an alternative solution for foreign institutions with diverse and deep data requirements.

From the perspective of data availability, there are fundamental differences in the cross-border transfer restrictions for different grades of data:

- Important data: Since it triggers strict statutory procedures such as security assessment, it is reasonably foreseeable that, regardless of whether the buyer is onshore or offshore, such data will be difficult to acquire and transfer cross-border in practice.

- General data: In principle, it can be procured without a security assessment. However, the direct cross-border supply of "sensitive general data" within this category may face obstacles due to the risk appetite of certain data vendors.

Accordingly, foreign institutions may consider establishing an onshore entity (e.g., an unlicensed WFOE whose primary business activities are data collection and processing) to procure data directly from onshore vendors. After completing localized data cleansing, desensitization, and integration onshore, the data can then be transferred to offshore affiliates in a legally compliant manner to support offshore trading strategies. In practice, some foreign institutions have already adopted this structure by setting up data companies onshore.

However, it is important to note that establishing an onshore entity also entails various burdens:

- Compliance and regulatory oversight: The onshore entity must fully comply with relevant Chinese laws and regulations, fulfill corresponding data security obligations, and be subject to supervision by domestic regulatory authorities.

- Infrastructure deployment: It requires the onshore deployment of IT infrastructure, systems, and servers, as well as the proper handling of the resulting data localization and security management issues.

- IP and technology protection: During onshore operations, the boundaries of cross-border sharing and intellectual property protection for core algorithms, trading models, and key technologies must be carefully managed.

- Operational costs: This includes not only the initial setup costs but also ongoing expenses related to human resources, operations, and compliance.

If you would like to know more information about the subjects covered in this publication, please contact:

Sandra Lu
+86 21 3135 8776
sandra.lu@llinkslaw.com

Lily Luo
+86 21 3135 8732
lily.luo@llinkslaw.com

Neil Zhao
+86 21 6043 3937
neil.zhao@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668

HONG KONG	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD