Legal Commentary

October 9, 2020

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

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Banking & Finance Law

PBoC Releases Guidelines for Financial Data Classification

Authors: TieCheng YANG | Yin GE | Ting ZHENG | Virginia QIAO

On 23 September 2020, the People's Bank of China ("**PboC**") issued the *Financial Data Security - Guidelines for Data Security Classification (JR/T 0197-2020)* (《金融数据安全 数据安全分级指南(JR/T 0197-2020)》) (the "**Financial Data Classification Guidelines**"). Based on the *Cybersecurity Law of the People's Republic of China*(《中华人民共和国网络安全法》) (the "**Cybersecurity Law**") and the existing data protection rules, the Financial Data Classification Guidelines put forward systematic and specific requirements in the field of data classification for financial institutions. In this legal commentary, we will analyze the key points of the Financial Data Classification Guidelines from the perspective of corporate compliance, with a focus on how the new requirements under the Financial Data Classification Guidelines overlay existing regulations and standards.

Background and principle of "data classification" - *What is the purpose for issuing the Financial Data Classification Guidelines?*

"Data classification" has been one of the key regulatory principles in the field of cybersecurity and data protection. In 2016, the Cybersecurity Law imposed a data classification requirement on network operators, among other security protection obligations. According to Article 21 of the Cybersecurity Law, enterprises, as network operators, are required to take data classification and other security protection measures to prevent data from being disclosed, stolen or tampered with. Furthermore, on 3 July 2020, the Standing Committee of the National People's Congress released a consultation draft of the *Data Security Law of the People's Republic of China* (《中华人民共和国数据安全法(草案)》), which proposed that an overall data protection system be established at the national level, in which data classification and classified protection requirements were specified.

In addition, PRC regulators released a series of consultation drafts which also defined compliance requirements for data classification, e.g., the *Regulations on Classified Protection of Cybersecurity (Consultation Draft)* (《网络安全等级保护条例(征求意见稿)》), the *Measures for Administration of Data Security (Consultation Draft)* (《数据安全管理办法(征求意见稿)》), the *Regulations for Security Protection of Critical Information Infrastructure (Consultation Draft)* (《关键信息基础设施安全保护条例(征求意见稿)》),

the *Information Security Technology - Implementation Guides for Data Security Classification (Draft)* (《信息安全技术 数据安全分类分级实施指南（草案）》), etc. There are separate industry-specific data classification guidelines formulated in manufacturing industry and other sectors.

In the financial sector, "data classification" is also a regulatory focus of financial regulators. In September 2018, the China Securities Regulatory Commission issued the *Data Classification Guidelines for Securities and Futures Industry (JR/T 0158-2018)* (《证券期货业数据分类分级指引(JR/T 0158-2018)》) (the "**Securities and Futures Data Classification Guidelines**") which mark the first data classification requirements for the financial sector. However, the applicable scope of the Securities and Futures Data Classification Guidelines only covers securities firms, futures companies and fund management companies.

On 13 February 2020, PBoC and the China Financial Standards Technical Committee issued the *Personal Financial Information Protection Technical Specification (JR/T 0171-2020)* (《个人金融信息保护技术规范(JR/T 0171-2020)》) (the "**Specification**"). The Specification adopts the regulatory principle of "data classification", and classifies the sensitivity of personal financial information into three types: C3, C2 and C1. We provided a detailed analysis on the Specification in our previous Han Kun Legal Commentary, Key Analysis on the Personal Financial Information Protection Technical Specification.

With the development of financial technology and the digital economy, financial data has demonstrated tremendous social and commercial value with increasing complexity. In this context, PBoC issued the Financial Data Classification Guidelines to provide detailed and practical guidance for data classification of financial institutions, helping them to better clarify the subjects of classified data protection, optimize resources and costs for data security protection, and further establish a sound financial data lifecycle management framework.

Expanded scope of "financial industry institutions" - *What is the scope of application of the Financial Data Classification Guidelines?*

The Financial Data Classification Guidelines define the scope of application as "institutions engaging in the financial industry" (collectively, "**Financial Industry Institutions**"), as defined in the *Industrial Classification for National Economic Activities (GB/T 4754-2017)* (《国民经济行业分类(GB/T 4754-2017)》).

As compared with the Securities and Futures Data Classification Guidelines, which cover securities firms, futures companies and fund management companies, the Financial Data Classification Guidelines expand to cover other financial institutions such as commercial banks, insurance companies, trust companies, etc. The Financial Data Classification Guidelines also apply to private fund managers (including institutions such as PFM, QDLP and QDIE), third-party payment companies, credit information agencies, etc. Additionally, due to the correlation between industries and the flexibility for interpreting the scope of application, the Financial Data Classification Guidelines may also have an indirect impact on institutions engaging in data security evaluation and assessment, such as third-party data evaluation agencies.

It is noteworthy that although the Financial Data Classification Guidelines and the Specification both apply to "financial industry institutions" from a literal reading, they define this term differently. Under the Specification, "financial industry institutions" include "licensed financial institutions supervised and regulated by the financial regulatory authorities in China, and the relevant institutions involved in the personal financial information processing", which means the Specification directly applies to licensed financial institutions including banking financial institutions, securities firms, fund management companies and insurance companies, as well as related institutions that process personal financial information (which may or may not be licensed), such as third-party payment companies, credit information agencies, etc. Additionally, although PFM/QDLP managers are not "licensed financial institutions" in a strict sense, if they process any customer's personal information in providing financial services, they should also observe the Specification as the "institutions processing personal financial information".

We set out below a table summarizing by different types of institutions the applicability of the Specification, the Securities and Futures Data Classification Guidelines and the Financial Data Classification Guidelines:

Type of institutions	Specification	Securities and Futures Data Classification Guidelines	Financial Data Classification Guidelines
Licensed financial institutions of securities and futures business (i.e. securities firms, futures companies, and fund management companies)	√ (Applicable to "personal financial information" processed by such institution)	√	**Optional** (The Securities and Futures Data Classification Guidelines could be followed instead)
Other licensed financial institutions (including commercial banks, insurance companies, trust companies, etc.)		×	√ (Applicable to "financial data" of institutions)
Private fund managers (including institutions such as PFM, QDLP and QDIE)			
Third-party payment companies			
Credit information agencies			

It should be noted that the Financial Data Classification Guidelines are only voluntary standards for the financial industry, rather than mandatory standards. While at the current stage the Financial Data Classification Guidelines are not compulsory in their application and retain a certain degree of flexibility, provisions of voluntary standards can, in practice, either be directly referenced in or integrated into subsequent compulsory provisions. We also do not rule out the possibility that the financial regulators may consider the Financial Data Classification Guidelines as an important reference when conducting relevant supervisory inspections or law enforcement actions, and may deem the Financial Data Classification Guidelines as practical guidance or operating guidelines for Financial Industry Institutions.

Therefore, we recommend that Financial Industry Institutions comply with the relevant standards and requirements as set out in the Financial Data Classification Guidelines to minimize any legal or compliance risks in relation to financial data classification.

Scope of "financial data" - *What are the financial data to be classified?*

The Financial Data Classification Guidelines focus on the classification of "electronic data" required or generated by Financial Industry Institutions in (i) carrying out business activities; (ii) providing financial services; and (iii) carrying out day-to-day operations and management. The financial data covered by the Financial Data Classification Guidelines include but are not limited to the following four types:

Type 1: Electronic data collected directly (or indirectly) by Financial Industry Institutions during the provision of financial products or services to clients.

Type 2: Electronic data generated and/or stored in the information systems of Financial Industry Institutions, including business information, transaction data, operation and management data, etc.

Type 3: Electronic data generated, transferred and/or stored in the internal office networks of Financial Industry Institutions, including administrative information, internal notices and e-mails, etc.

Type 4: Electronic data generated from the original paper-based documents of Financial Industry Institutions through scanning or other electronic means.

It should be noted that the Financial Data Classification Guidelines do not cover data which constitutes "state secrets". Financial data involving "state secrets" is instead handled in accordance with the relevant national laws and regulations promulgated by the relevant PRC authorities in respect of state secrets' protection, e.g., the *Law of the People's Republic of China on Guarding State Secrets* (《中华人民共和国保守国家秘密法》), the *Regulations for the Implementation of the Law of the People's Republic of China on Guarding State Secrets* (《中华人民共和国保守国家秘密法实施条例》), the *Interim Provisions on Administration of Classifying State Secrets* (《国家秘密定密管理暂行规定》), etc.

Standards on financial data classification - *How will financial data be classified?*

Similar to the Securities and Futures Data Classification Guidelines, the Financial Data Classification Guidelines adopt a multi-level data classification system based on the two key indicators of "impacted areas" and "degree of impact". According to the Financial Data Classification Guidelines, Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, in descending order of importance, by evaluating the "impacted areas" and the "degree of impact" in the event of data leakage or destruction.

Among others, "impacted areas" include national security, public rights and interests, personal privacy, legitimate rights and interests of enterprises, etc. "Degree of impact" could be measured as "serious damage", "ordinary damage", "minor damage" or "no damage". Financial Industry Institutions may carry out data classification by reference to the following matrix:

Minimum level	Key indicators for data classification		Key features and examples
	Impacted area	Degree of impact	
5	National security	Serious damage/ordinary damage/minor damage	■ “Important data” of Financial Industry Institutions. ■ Used for critical business activities of large or ultra-large Financial Industry Institutions and key financial trading platforms. ■ Disclosed to specific personnel on a “need-to-know” basis only.
	Public rights and interests	Serious damage	
4	Public rights and interests	Ordinary damage	■ Used for important business activities of large or ultra-large Financial Industry Institutions and key financial trading platforms. ■ Disclosed to specific personnel on a “need-to-know” basis only. ■ **Personal financial information (C3)** under the Specification.
	Personal privacy	Serious damage	
	Legitimate rights and interests of enterprises	Serious damage	
3	Public rights and interests	Minor damage	■ Used for critical and important business activities of Financial Industry Institutions. ■ Disclosed to specific personnel on a “need-to-know” basis only. ■ **Personal financial information (C2)** under the Specification.
	Personal privacy	Ordinary damage	
	Legitimate rights and interests of enterprises	Ordinary damage	
2	Personal privacy	Minor damage	■ Used for general business activities of Financial Industry Institutions. ■ Disclosed to a specific scope for internal use only. ■ **Personal financial information (C1)** under the Specification.
	Legitimate rights and interests of enterprises	Minor damage	
1	National security	No damage	■ Disclosed to or accessible by the public. ■ Voluntarily disclosed by the natural person subjects of personal financial information themselves.
	Public rights and interests	No damage	
	Personal privacy	No damage	
	Legitimate rights and interests of enterprises	No damage	

It is noteworthy that Schedule A (*Table of Data Classification Rules*) of the Financial Data Classification Guidelines further provides a comprehensive summary of data samples and their corresponding levels for data classification. Detailed evaluation standards are further provided in the Financial Data Classification

Guidelines.

Process of financial data classification - *How would Financial Industry Institutions carry out data classification?*

Based on overall data classification process set out in the Financial Data Classification Guidelines, Financial Industry Institutions should themselves internally determine and approve data security classifications. The Financial Data Classification Guidelines specify the internal process for data security classifications covering the following five steps:

Step 1 (Formulation of data asset inventory)
■ Review and sort electronic data of the institution ■ Develop a unified inventory of data assets
↓
Step 2 (Preparation for data security classification)
■ Determine the granularity of data classification ■ Identify key data security classification elements
↓
Step 3 (Determination of data security levels)
■ Determine data security levels ■ Formulate separate data inventories at different security levels
↓
Step 4 (Review of data security levels)
■ Check and review the whole process and results of data security classification
↓
Step 5 (Approval of data security levels)
■ Final approval of data security levels by the institution’s highest decision-making body

According to the Financial Data Classification Guidelines, a Financial Industry Institution should determine its “highest decision-making body” for data security classification, e.g., set up a data security management committee for the institution. In addition, a Financial Industry Institution should define an organizational structure, with clear roles and responsibilities divided among its departments and staff. No regulatory approval is required for the data classification results at the current stage.

Data protection requirements - *How would Financial Industry Institutions protect their financial data?*

According to the Financial Data Classification Guidelines, Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, in descending order of importance. Comparatively, the

Specification divided the sensitivity levels of personal financial information into three types: C3, C2 and C1. Although the Financial Data Classification Guidelines do not directly set data protection requirements for Financial Industry Institutions, it is noteworthy that the Financial Data Classification Guidelines specify correlations with the Specification, namely:

1. C3 data under the Specification should correspond with Level 4 data under the Financial Data Classification Guidelines;
2. C2 data should correspond with Level 3 data; and
3. C1 data should correspond with Level 2 data.

In light of the above, upon determination of the data classification from Level 1 to Level 5, Financial Industry Institutions should observe by reference the corresponding data protection requirements as set out in the Specification, for instance:

1. Financial Industry Institutions should refrain from appointing or authorizing any institutions without the relevant financial licenses to collect C3 or C2 information. To collect C3 information, relevant technical measures such as encryption should be taken to prevent any unauthorized third party from obtaining such information;
2. to transmit sensitive payment information among C3 information, Financial Industry Institutions should adopt relevant control measures that conform to industry technical standards as well as the requirements of industry authorities;
3. in principle, a Financial Industry Institution should not retain C3 information which it does not own. Where there is a specific need, such retention should be authorized by the information subjects and the account management institutions;
4. in principle, Financial Industry Institutions should refrain from appointing third-party institutions to process C3 personal financial information and auxiliary user identification information (such as text message verification codes) among C2 personal financial information;
5. C3 information or auxiliary user identification information among C2 information should not be shared, transferred or disclosed; and
6. outsourcing service institutions and external cooperation institutions should be prohibited from retaining C3 and C2 information by contract or agreement.

Outlook - *What do we expect regarding regulatory trends?*

Compared with the existing laws and regulations, the Financial Data Classification Guidelines are more practical and thus can play an important guiding role in compliance practices for Financial Industry Institutions, which may further lay the foundation for standardized data protection and data lifecycle management in the financial industry. We anticipate that PBoC and other financial regulators may formulate and issue detailed implementing rules in this regard.

In addition, although the Financial Data Classification Guidelines fill the gap in classified data management and mark a further step in the data protection rules, financial regulators have further room for rulemaking. For instance, although Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, the Financial Data Classification Guidelines do not provide data protection requirements for each level of financial data, which may be further specified in subsequent regulatory rules or national/industry standards.

With the continuous development of the regulatory framework on data lifecycle management and personal information protection in China, we will also continue to monitor relevant regulatory updates and share our views with readers in a timely manner.

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:

TieCheng YANG

Tel: +86 10 8516 4286
Email: tiecheng.yang@hankunlaw.com

Yin GE

Tel: +86 21 6080 0966
Email: yin.ge@hankunlaw.com