Legal Commentary

May 23, 2025

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

BEIJING | SHANGHAI | SHENZHEN | HONG KONG | HAIKOU | WUHAN | SINGAPORE | NEW YORK

Key Implications of PBoC Data Measures and Actions

Authors: Ting ZHENG | Eryin YING | Lin ZHU | Shirley LIANG | Hattie ZHANG

Overview

On 9 May 2025, the People's Bank of China (**PBoC**) issued the *Measures for the Administration of Data Security in the Business Areas of the People's Bank of China* (《中国人民银行业务领域数据安全管理办法》) (the "**PBoC Data Measures**") which shall take effect on 30 June 2025. The PBoC Data Measures and the PBoC's Q&A on the PBoC Data Measures (available in Chinese only) can be accessed on PBoC's website at: *http://www.pbc.gov.cn/tiaofasi/144941/144957/5702602/index.html* and *http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/5706206/index.html*.

The PBoC Data Measures are PBoC's first comprehensive regulation specifically addressing data security under PBoC's business areas. We summarize below the key requirements, implications and recommended actions of such rules, especially on financial institutions such as commercial banks.

Key implications

I. Applicable scope

1. Applicable data processing activities

The *Data Security Law of the People's Republic of China* (《中华人民共和国数据安全法》, the "**DSL**") explicitly provides that sector-specific regulators, including financial authorities, are responsible for supervising data security within their respective industries and areas. In line with such principle, PBoC Data Measures apply to the **onshore processing activities of data within PBoC's business area, which is defined as network data generated or collected within PBoC's business areas but excluding state secret**.

(a) Network data

According to Article 62 of the *Regulation on Network Data Security Management* (《网络数据安全管理条例》), "network data" shall refer to various electronic data handled and generated through networks. Therefore the data within PBoC's business area excludes non-electronic data, such as data on paper documents.

(b) State secret

In line with Article 53 of the DSL, state secret is expressly excluded from the scope of data within PBoC's business area. Any processing of state secret shall be subject to 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》) and relevant implementation rules.

(c) PBoC's business area

According to the PBoC's Q&A on the PBoC Data Measures, "PBoC's business areas" refer to areas in which the PBoC performs supervisory and administrative functions, including monetary credit, macro-prudential management, cross-border RMB business, the interbank market, comprehensive statistics and analytics of the financial industry (金融业综合统计), payment and clearing, RMB issuance and circulation, treasury operations, credit reporting and credit rating, and anti-money laundering, among others.

2. Applicable data processors

The PBoC Data Measures are widely applicable to **both financial institutions and other institutions that are either established under the approval of PBoC or recognized by PBoC**. While there is no further clarification by PBoC regarding the scope of applicable data processors, from a prudent perspective and in view of the regulated scope of data within PBoC's business area, all financial institutions and other regulated institutions that process data within PBoC's business area may potentially fall in the scope of the data processors under the PBoC Data Measures.

II. Data classification (数据分类) and grading (数据分级)

Article 7 of the PBoC Data Measures requires data processors to establish and improve data classification and data grading policies and implementation procedures. Articles 8 and 9 go further to specify PBoC's standards for data classification and grading.

1. Data classification

PBoC Data Measures introduce a three-dimensional approach to data classification — **business relevance, sensitivity, and availability**.

(a) Business relevance

The data within PBoC's business area should be classified based on whether the data is personal information, whether the data is collected or generated from external sources, the list of information system storing such data, and the business category relevant to such data, each of which should be labeled on the relevant data.

(b) Sensitivity

The data within PBoC's business area should be classified based on the extent of harm caused to the legitimate rights and interests of individuals and organizations or public interests when the data is leaked, illegally acquired or illegally used.

In the course of data classification, for structured data items, data processors shall identify and label the sensitivity of each structured data item; for unstructured data items, data processors shall identify and label with priority the sensitivity of such unstructured data item according to the highest sensitivity of structured data items that can be split out from such unstructured data item.

Notably, sensitive personal information, clients' business information that may involve business secrets and business information the access to which should be strictly controlled, shall be identified and labeled as highly sensitive data items.

(c) Availability

The data within PBoC's business area should be classified based on the degree of impact on normal business operations caused by falsification or destruction of the data and the resulting differentiated data recovery point objectives of information system.

2. Data grading

The PBoC's Data Measures have followed the same grading mechanism in the DSL, i.e., the data is graded into **core data, important data and general data**. Data processors shall submit their important data catalog to PBoC and PBoC will feedback the scope of important data processed by data processors. Data processors can refer to the *Financial Data Security — Guidelines for Data Security Grading* (金融数据安全 数据安全分级指南) for further guidance on the data grading.

Data processors shall classify and grade their data within PBoC's business area pursuant to the above classification and grading requirements, and formulate their data catalog, which shall be **updated at least annually**.

III. Whole lifecycle data security management and technical requirements

Chapter 3 and 4 of the PBoC Data Measures provide for comprehensive and differentiated data security management and technical requirements applicable to different classified and graded data. Overall, these data security management and technical requirements are consistent with those provided for in the *Financial Data Security — Security Specification of Data Life Cycle* (金融数据安全 数据生命周期安全规范) and do not impose overly burdensome requirements. Below is a summary of key requirements:

Data processing activity	Management requirement	Technical requirement
Collection	■ Obtaining informed consent or authorization from data subjects (Art.15); ■ For indirect data collection, specifying the obligation of the data provider to ensure the legality and authenticity of data source; where the data provider fails to obtain the written consent or	■ Prioritizing data collection via direct input or interaction between information systems. Verifying the inputter' identity for direct input, and data provider's identity for collecting highly sensitive data item via information system interaction (Art.31); ■ Ensuring data accuracy via

Data processing activity	Management requirement	Technical requirement
	authorization of data subjects, it shall be required to provide the necessary supporting materials for the legality and compliance of the data source and the authenticity of the data (Art.15); ■ No collection of original personal biometric information in principle (Art.15); ■ Complying with the contracts with data provider for data collection and processing (Art.15).	information cross check (Art.31); ■ No interruption to normal operation when collecting data via automatic tools (Art.31).
Storage	■ Specifying storage period (Art.16); ■ No storage of highly sensitive data item on terminal equipment or mobile media in principle (Art.16).	■ Separating test environment from production environment (Art.32); ■ Information system meeting the level-3 protection requirements if storing important data, and level-4 protection requirements if storing core data (Art.32); ■ Storing highly sensitive data items in an encrypted manner (Art.32); ■ Verifying availability of data backup (Art.32).
Use	■ No export of highly sensitive data item in principle (Art.17); ■ Display of highly sensitive data item after data masking in principle (Art.17); ■ Using verification method for identity authentication in principle (Art.17).	■ Specifying data mask strategy of highly sensitive data items (Art.33); ■ Identifying current account and use time when displaying or printing data (Art.33); ■ Internal approval and data masking when using data from production environment for test environment (Art.33).
Process	■ Processing in consistency with the agreed purpose (Art.18); ■ Focus on data quality (Art.18); ■ Additional security requirements for highly sensitive data items (Art.18); ■ Level up or down in the sensitivity of new data generated from data processing activity (Art.19).	■ Maintaining the security of algorithms for data processing (Art.34).

Data processing activity	Management requirement	Technical requirement
Transmission	■ No transmission of highly sensitive data items via internet information services or mobile media, except for transmission to individuals upon their request (Art.20).	■ Prioritizing the use of special lines or VPN for data transmission (Art.35); ■ Improving access control and separation strategy (Art.35); ■ Transmitting highly sensitive data items in an encrypted manner in principle (Art.35); ■ Evaluating transmission capacity of lines and enhancing backup (Art.35).
Provision	■ Verifying data receiver's identity (Art.21); ■ Assessing compliance with applicable laws or contractual agreement on keeping trade secret (Art.21); ■ Specifying contractual data security protection obligations and monitoring the compliance (Art.21); ■ Prior risk assessment before provision, entrusted processing or joint processing of important data (Art.22); ■ Prior risk assessment before provision of core data (Art.22); ■ Required terms in the agreement with each service provider for entrusted process (Art.28); ■ Prior due diligence into each entrusted service provider (Art.28).	■ Dynamically maintaining the front-end gateways and application interfaces for data provision, carrying out security test before putting into operation (Art.36); ■ Establishing technical risk assessment and control strategy when providing data via privacy computing (Art.36).
Innovative application of data integration	■ Same requirements for data provision above (Art.23); ■ Ensuring no other data processor can use unencrypted original data and ensuring no leakage of information beyond the agreed scope (Art.23).	N/A
Outbound transfer	■ Requisite procedures for outbound transfer in existing rules (Art.24);	N/A

Data processing activity	Management requirement	Technical requirement
	■ Storing data onshore if required (Art.24).	
Publication	■ Internal approval for data publication (Art.26); ■ No publication of data items for identity authentication, and masking of other highly sensitive data items (Art.26).	■ Formulating control rules on the permissibility of data collection via automatic tools (Art.37); ■ Adopting necessary technical measures to ensure the data from being tampered with (Art.37).
Deletion	■ Deleting data upon specified circumstances (Art.27); ■ At least annual review to ensure un-usability of deleted data (Art.27).	■ Specifying the destroy strategy and procedure of data storage media (Art.38).
Access control	■ Strict management of access control of accounts (Art.14); ■ Entering into confidentiality agreements with personnel that have access to highly sensitive data items (Art.14); ■ Security background check on security responsible person and key personnel having access to core data, if the data processor stores core data (Art.14).	■ Enhancing access control by adopting technical measures (Art.29); ■ Internal approval and authorization for the use of privileged account (Art.29); ■ Establishing multi-factor authentication or secondary authorization mechanism for accounts that can use highly sensitive data items (Art.29); ■ Establish re-authentication mechanism (Art.29).
Data processing log	N/A	■ Including data processing log into data classification and grading management (Art.30); ■ Requiring retention period for data processing log, which shall be at least one (1) year for important data storage related log, at least three (3) years for core data storage related log, and at least three (3) years for personal information provision, entrusted processing and important data processing activity related log (Art.30).

IV. Data security risks and incidents management

Chapter 5 of the PBoC Data Measures sets out requirements for **risk monitoring, alert and early warning mechanisms, assessment and audit, classification of incidents, and emergency response**. The following key requirements are particularly note-worthy:

1. Assessment

Article 42 of the PBoC Data Measures requires that important data processors shall, either on their own or by engaging a third-party assessment agency, conduct a risk assessment of their data at least once a year, and submit the risk assessment report for the previous year to PBoC or its provincial branch at their place of registration by 15 January each year. Article 42 further provides that, in addition to the matters that are already explicitly required to be assessed under laws and administrative regulations (primarily Article 31 of the *Regulation on Network Data Security Management*), the **risk assessment report must additionally include the following**:

(a) training and day-to-day management relating to the information systems used for storing important data;

(b) implementation of role-based responsibilities related to business data;

(c) status of cybersecurity graded protection assessment and rectification;

(d) implementation of protective measures;

(e) risk monitoring and incident handling undertaken during the year; and

(f) any other assessment items required by PBoC.

2. Grading of data security incidents

Article 43 of the PBoC Data Measures requires data processors to grade data security incidents according to the *National Contingency Plan for Cyber Security Incidents* (《国家网络安全事件应急预案》) issued by the Cyberspace Administration of China (**CAC**), and specify the grading standard for data security incidents. Notably, the annex to the *Administrative Measures for Data Security of Banking and Insurance Institutions* (《银行保险机构数据安全管理办法》, the "**NFRA Data Measures**") also provide for the grading standard of data security incidents, which is similar to the standard provided by CAC. The data security incidents are graded into extremely serious data security incidents, serious data security incidents, relatively serious data security incidents, and general data security incidents. Data processors should properly incorporate these grading mechanisms in their own internal policies.

3. Emergency response

Article 44 of the PBoC Data Measures requires data processors to take handling measures immediately upon the occurrence of data security incidents, inform clients and report to PBoC. While the PBoC Data Measures do not specify the timeline for report to PBoC, data processors may refer to the *Administrative Rules for Reporting of Computer Security Incidents of Banks* (《银行计算机安全事

件报告管理制度》) for reference, i.e., report to the local office of PBoC within twelve (12) hours from the occurrence of the incident.

4. Emergency drill

According to Article 44 of the PBoC Data Measures, important data processors shall conduct emergency drill for data security incidents at least once a year, and other data processors shall conduct emergency drill at least once every three (3) years. Notably, the *Cybersecurity Law of the People's Republic of China* (《中华人民共和国网络安全法》) and NFRA Data Measures also require periodic emergency drills but do not provide for frequency requirement.

5. Audit

Article 45 of the PBoC Data Measures requires data processors to conduct a business data security compliance audit at least once every three (3) years, and important data processors to conduct a compliance audit on important data security at least once every year. A special audit is further required after the occurrence of a serious or extreme serious data security incident. Article 45 of the PBoC Data Measures also provides for the contents to be focused on in the audits.

Outlook

The release of the PBoC Data Measures marks a giant step in the regulation of processing activities of data within PBoC's regulated sphere, and provides clearer guidance on meeting baseline data security compliance requirements of PBoC. However, it also presents significant practical compliance challenges for those institutions that are subject to regulation of multiple authorities, e.g., commercial banks will need to comply with both the PBoC Data Measures and NFRA Data Measures during its business operation. Our team are quite experienced in data compliance projects of financial institutions, especially banks, and will be more than happy to help our clients to develop a unified and practical data governance framework aligned with these evolving requirements.

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:

Ting ZHENG

Tel: +86 21 6080 0203
Email: ting.zheng@hankunlaw.com