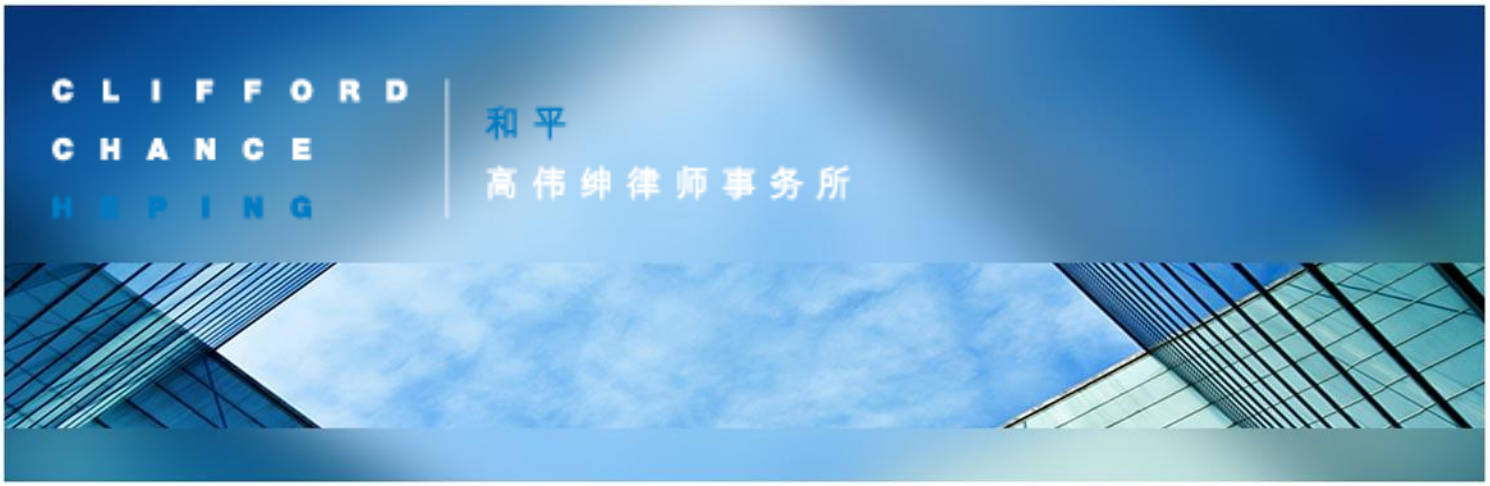

THE PEOPLE'S BANK OF CHINA DATA AND CYBER SECURITY MEASURES: PRACTICAL COMPLIANCE GUIDE FOR FINANCIAL INSTITUTIONS

OVERVIEW

The People's Bank of China[1] ("**PBOC**") released (i) *the Regulations on Data Security in PBOC Business Areas* (the "**PBOC Measures**"), which will be effective from 30 June 2025 and (ii) *the Measures on Cybersecurity Incident Report in PBOC Business Areas* (the "**PBOC Incident Reporting Measures",** collectively with the PBOC Measures, the "**PBOC Rules**"), which will be effective from 1 August 2025.

The PBOC Rules implement China's core data protection laws (*i.e.,* the PRC Cybersecurity Law (2017), the PRC Personal Information Protection Law (2021) and the PRC Data Security Law (2021)) within PBOC-supervised sectors. Importantly, these rules set forth clear and actionable requirements on in-scope institutions, with detailed instructions. Given PBOC's central role, these measures will likely serve as a benchmark for broader data/cyber governance regimes in China's financial sector.

This briefing discusses the key compliance obligations under the PBOC Rules and their potential implications for businesses operating under PBOC's supervision.

SCOPE OF APPLICATION

The PBOC Measures apply to data processing activities in China (i) by financial institutions and other PBOC-approved or recognised entities and (ii) that relate to areas supervised by PBOC. The scope of application of PBOC Incident Reporting Measures is straightforward – they apply only to institutions that are approved or recognised by PBOC with respect to their cybersecurity incident management.

In-scope institutions

The PBOC Measures do not explicitly define 'financial institutions' subject to these rules. A potential interpretation is that covered entities could include any institution licensed by a financial regulator, i.e., the National Financial Regulatory Administration ("**NFRA**"), the China Securities Regulatory Commission ("**CSRC**") and PBOC itself. A financial institution might therefore

Key Takeaways

- The PBOC Measures reinforce existing data laws while signaling PBOC's role in shaping China's financial data governance, which will influence the wider industry approach.
- The PBOC Measures clarify approach to data classification, and also mandate detailed data inventorying, tagging, and DSL-aligned grading.
- The PBOC Measures introduce more detailed, actionable compliance requirements covering the full life-cycle of data.
- The PBOC Incident Reporting Measures require financial institutions to classify incidents into four levels and follow specific reporting procedures, including immediate, ongoing, and post-incident reports, with timelines varying based on the severity of the incident.
- Financial institutions may face overlapping regulatory regimes and further alignment work will be required.

[1] "**China**" or the "**PRC**" means the People's Republic of China. This briefing concerns PRC law only, without accounting for laws that are applicable to the Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan Region respectively. The geographic jurisdiction scope shall be interpreted accordingly.

be simultaneously subject to data protection rules of NFRA/CSRC[2] and the PBOC Measures, depending on their activities.

Entities that are not licensed in China could also be subject to these measures if they are 'recognised' by PBOC. It remains to be seen how this will be applied in practice, in particular to non-PRC entities that obtained recognition or approval from PBOC (or perhaps only made a filing).

Third-party service providers (e.g. SaaS vendors) are not directly regulated under the PBOC Measures. However, they may become subject to indirect compliance obligations through contractual requirements imposed by in-scope institutions.

In-scope data

The PBOC Measures cover data processing activities tied to "PBOC-supervised business areas." PBOC's accompanying press release specifies that these areas include: monetary and credit policies, macroprudential management, cross-border RMB business, interbank markets, financial statistics, payment and settlement, RMB issuance and circulation, treasury management, credit reference and credit rating, anti-money laundering, and other areas supervised by PBOC.

PRACTICAL APPROACH TO DATA CLASSIFICATION

The *PRC Data Security Law* (2021) ("**DSL**") mandates that data processors must apply tiered protection measures based on data classification, with important data and core data attracting more stringent protection. The financial services industry, like others, has since been exploring how this requirement should be implemented in practice.

In this regard, the PBOC Measures now provide detailed operational guidance on how data should be classified, which can be summarised as follows:

1. **Data inventory**: in-scope institutions must maintain an up-to-date inventory of data stored in their information systems, and keep such inventory updated at least annually;
2. **Data tagging**: each data item must be tagged based on its relevance, sensitivity and availability:
    (a) relevance: data must be tagged to indicate whether it constitutes personal information, whether it is externally sourced, the list of information systems where it is stored, and to which businesses such data items relate;
    (b) sensitivity: data must be tagged with its sensitivity, i.e., the level of harm from leakage or illegal use of such data. Specifically –
        (i) structured data and unstructured data[3] will involve different tagging approaches: structured data should be tagged individually, whereas unstructured data should be firstly decomposed into constituent structured data items, which shall be tagged

[2] NFRA and CSRC have issued data security rules that apply to institutions subject to their respective oversight, i.e., the NFRA Rules on Data Security of Banking and Insurance Institutions (2024), and the CSRC Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industries (2023)

[3] Broadly speaking, structured data mean data that are highly organised, formatted and easy to process through data processing tools and are normally presented in two-dimensional databases, *e.g.*, names, dates, addresses, credit cards numbers; whereas unstructured data is often categorised as qualitative which cannot be processed and analysed through conventional data tools and methods, e.g., pictures, videos, audio, document files.

individually, and the sensitivity level of the unstructured data will be the highest level among the constituent structured data units;

(ii) sensitive personal data, client business information that could involve commercial secrets and other business data subject to strict disclosure control should be applied with a high-sensitivity tag; and

(c) availability: data should also be tagged based on the potential impact on business continuity if the relevant data item is compromised or destroyed.

3. **Data grading**: consistent with the DSL, data should be classified into general data, important data and core data; and PBOC is responsible for formulating a catalogue of what constitutes important data. A welcome development is that PBOC will launch an initiative to identify important data and notify processors of the identified important data. In other words, only formally-identified entities will be subject to enhanced obligations on important data under the PBOC Measures.

4. **Data protection**: data processors should have technical and organisational measures to protect data, and the level of protection should be designed based on the classification of data following the approach outlined above.

It should be noted that the financial services sector currently uses a five-tier data classification system to describe data security levels.[4] While the consultation draft of the PBOC Measures adopted a five-tier approach to measure data sensitivity, the finalised version did not retain it. We understand work is underway to harmonise the five-level approach with the DSL's three-tier framework (general–important–core), as implemented by the PBOC Measures.

INTERNATIONAL DATA TRANSFER

International data transfer is a common concern for multinational companies operating in China, particularly due to the international nature of business, shared group systems or functions supported by group entities. The PBOC Measures may impact international data transfer arrangements in the following ways.

Compliance with existing regimes

The PBOC Measures reaffirm that all data exports must comply with existing regulatory requirements[5]. They emphasise that data processors must not circumvent data export rules through data splitting or transformation.

That said, we understand this requirement does not intend to prohibit the use of legitimate privacy enhancing technologies so that the data being transferred no longer constitutes personal data or important data.

More detailed requirements

The PBOC Measures introduce more detailed rules on data transfers, which also apply to international transfers. Key requirements include -

(a) **High-sensitivity data restrictions**: unless for entrusted processing, in principle it is prohibited to provide high sensitivity data to any data

[4] See the Financial Data Security – Guidelines for Data Security Classification (JR/T 0197-2020).

[5] See our briefing (here) on China's current rules governing international data transfer.

recipient through an "export-based transfer method" (*i.e.*, converting data with strict access controls to document files without such controls);

(b) **Entrusted processing agreements**: for entrusted processing, while there is no industry-wide template, the PBOC Measures prescribe an agreement that contains specific terms (*e.g.*, reporting obligation of the entrusted party, data deletion and data retention requirements);

(c) **Data received from a third-party**: where the in-scope institution receives non-public data from another party, it needs to obtain from the provider a representation that the data is legitimately sourced and accurate.

Crucially, in-scope institutions must accurately characterise the legal relationship between the parties to a data transfer (*e.g.*, entrusted processing, data sharing or joint processing), which in turn determines the compliance obligations that will apply.

Integrating data governance into outsourcing framework

In-scope institutions must integrate entrusted processing into their outsourcing frameworks. If a function or business activity is prohibited from being outsourced, then the related data transfer must also be prohibited.

Financial institutions must implement robust systems and controls to manage outsourcing risks – which is a long-standing requirement now gaining increasing regulatory attention given the advancement of technologies. The PBOC Measures mean, at a minimum, that in-scope institutions must enforce controls over their outsourcing service provider (which could be a group entity) under both outsourcing as well as data regulations.

CYBERSECURITY INCIDENT MANAGEMENT

The PBOC Measures mandate strict incident management, requiring institutions to: (i) classify events by severity (considering data sensitivity, impact scope, and system recovery factors); (ii) report breaches (see below); and (iii) conduct emergency drills (at least annually for important data processors and triennially for others).

The PBOC Incident Reporting Measures provide details on the exact reporting procedures an in-scope institution must follow, which are summarised below:

Incident level / Steps	Extremely Severe (特别重大)	Severe (重大)	Material (较大)	General (一般)
Classification	In-scope institutions must classify the incident into four levels (following the internal procedures formulated by each in-scope institution pursuant to the PBOC Incident Reporting Measures) and take the corresponding course of action			
Immediate report	In-scope institutions should submit – 1. a brief report within 1 hour upon occurrence of the incident; and 2. a full incident report within 24 hours upon occurrence of the incident.			N/A, unless the incident attracts significant public or media attention, in which case follow the steps for material or above incidents
On-going report	In-scope institutions should submit – 1. an update report every 2 hours until the incident response procedures are completed; and 2. an ad-hoc report immediately upon occurrence of any critical developments.		/	/
Post-incident report	In-scope institutions should submit a post-incident investigation and summary report within 10 working days after completion of the cybersecurity incident response, subject to an extension of up to 40 working days.			

ADDITIONAL COMPLIANCE REQUIREMENTS

The PBOC Measures contain extensive provisions beyond those discussed above. While not exhaustive, the following requirements merit particular attention:

1. **Compliance audits**: in-scope institutions must conduct business data security compliance audits at minimum every three years, with important data processors required to conduct annual audits. Special audits must be performed following any major incident or particularly significant data breach;
2. **Use of external algorithm models**: when employing external algorithm models, in-scope institutions must ensure that raw data remains under their control. Particular vigilance is required to prevent unauthorised data linkage or scope expansion – this could be particularly relevant where a financial institution uses its data to fine-tune or train their own AI models; and
3. **Confidentiality agreements**: in-scope institutions should execute confidentiality agreements with employees who have access to highly sensitive data items. Given the explicit requirement for a confidentiality agreement, general confidentiality provisions in the employee handbook or other internal policies, for example, may not be sufficient to satisfy this requirement.

Conclusion

The PBOC Rules are critical regulations that establish an overarching data/cyber security framework as well as compliance standards for financial institutions. As China's legal framework for data/cyber security matures, the financial industry is entering a new phase of growth underpinned by robust regulatory safeguards. Regulators are now introducing clear and actionable requirements that financial institutions must adopt, laying the foundation for financial institutions to utilise the full potential of emerging technologies and the digital economy in a secure manner.

CONTACTS

SHANGHAI HE PING LAW FIRM

Kimi Liu
International Partner

T +86 21 5116 7212
E kimi.liu
@cliffordchancehp.com

Christine Li
Senior Associate

T +86 21 5116 7212
E christine.li
@cliffordchancehp.com

CLIFFORD CHANCE

Terry Yang
Partner

T +852 2825 8863
E terry.yang
@cliffordchance.com

Jane Chen
Senior Associate

T +86 10 6535 2216
E jane.chen
@cliffordchance.com

Jessy Cheng
Senior Associate

T + 86 10 6535 4935
E jessy.cheng
@cliffordchance.com

Shuai Gao
Associate

T + 86 10 6535 4915
E shuai.gao
@cliffordchance.com