24 August 2023

People's Bank of China
32 Cheng Fang Street
Xi Cheng District
Beijing 100800

To the People's Bank of China

Draft Measures for the Management of Data Security in People's Bank of China Business Areas

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] ("**we**", "**our**" or "**us**") are pleased to submit this letter to the People's Bank of China ("**PBOC**"). We seek to convey industry's views on the draft Measures for the Management of Data Security in People's Bank of China Business Areas ("**Draft Measures**"), and offer constructive ideas on how the Draft Measures can be refined to encourage foreign investment into the People's Republic of China ("**PRC**" or "**China**"), enhance risk management and facilitate compliance by financial institutions ("**FIs**") with robust standards and obligations aligned with those of other jurisdictions that are considered integral to world markets.

Summary of key concerns

1. Scope of application

(1) Unclear definition of "data processors"

Article 2 of the Draft Measures provides that data processors engaged in data-related processing activities in business areas regulated by PBOC are subject to the Draft Measures. Article 55(6) further defines "data processors" as FIs and other institutions that engage in data processing activities.

However, the exact nature of in-scope "data processors" cannot be definitively identified. For example:

(a) with respect to "FIs", does it refer to any FIs that are defined in a specific industry rule,

[1] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading FIs from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

ASIFMA - Unit 3603, Tower 2 Lippo Centre
89 Queensway Admiralty, Hong Kong

such as the *PBOC Regulations on Financial Institution Code (《金融机构编码规范》)*, or only those that are licensed by (i) PBOC or (ii) all PRC financial regulators (including PBOC, the National Administration of Financial Regulation ("**NAFR**") and the China Securities Regulatory Commission ("**CSRC**"), the latter option thereby covering banks, trust companies, securities firms, fund management companies, etc., as long as these organisations engage in business regulated by PBOC?

(b) does it apply to private asset managers registered with the Asset Management Association of China, such as Qualified Domestic Limited Partners (which are typically not considered to be FIs according to the general understanding of the industry)? In addition, does it apply to fund custodians or fund administrators registered with the Asset Management Association of China?

(c) there is no clarification of what kind of "other institutions" fall into the scope of the Draft Measures.

We urge PBOC to clarify in any revised version of the Draft Measures the scope of application of these measures in respect of in-scope organisations. In particular, on the basis that other regulators may look to release similar rules to the Draft Measures on data security for their own verticals of supervision, we would recommend that the scope of the Draft Measures is as narrow as possible to achieve the PBOC's objectives.

(2) Unclear definition of the "business areas of PBOC"

Article 2(2) of the Draft Measures provides that in-scope data are those "generated and collected in the course of various business activities for which the People's Bank of China assumes the responsibility of supervision and management". However, there is no detailed clarification on what the "business areas of PBOC" refers to under the Draft Measures. The *Drafting Instructions on the Draft Measures* (*《中国人民银行业务领域数据安全管理办法（征求意见稿）》起草说明*,"**Drafting Instructions**") explain that such business areas may cover "monetary policy business, cross-border RMB business, various interbank market transaction businesses, comprehensive financial industry statistics business, payment and settlement business, currency management and digital RMB business, treasury management business, credit reporting business, anti-money laundering business, etc." Considering this term is critical for identification of the application scope of the Draft Measures, we recommend that PBOC provides clarification in the Draft Measures on the meaning of this term (rather than in the Drafting Instructions alone).

(3) Extraterritoriality

Article 2 of the Draft Measures states that data processing activities carried out within the territory of the PRC are subject to the Draft Measures. On that basis, we understand the Draft Measures are not intended to have extraterritorial effect.

However, Article 13 states that in case of data processing activities conducted jointly with data processors having an affiliated relationship with such entities as parent companies, branches, affiliates or subsidiaries, the requirements for security protection management and technical measures must not be lowered. In this scenario, it seems the onshore data processors' foreign affiliates also need to comply with the Draft Measures to some extent.

We recommend that further clarification is provided regarding whether and how PBOC's supervision of foreign affiliates would be implemented under the Draft Measures in the context of jurisdictional sovereignty and the organisations that PBOC is not ordinarily authorised to regulate.

2. Data categorisation and classification

(1) New and multiple categorisation and classification requirements result in heavy operational burden

In general, the data categorisation and classification requirements as currently stipulated under the Draft Measures are onerous for FIs, especially considering all data processed by an FI in connection with the applicable business areas (albeit we recommend this to be clarified) would be in-scope.

We understand that the Draft Measures propose one set of data categorisation criteria and three sets of data classification criteria – i.e., Article 7 imposes an obligation to categorise data to create a data inventory, while for data classification, (i) under Article 8, data must be classified into three levels of general data, important data and core data; (ii) under Article 9, data must be classified into five levels based on sensitivity; and (iii) under Article 10, data must be classified based on data availability (although the detailed criteria/factors for classifying data based on availability remain unclear).

Based on their practical experience and practices in other markets, our members' view is that being required to adopt different sets of data categorisation/classification requirements with different criteria would overly complicate the data categorisation/classification process for both FIs and the competent authorities that supervise them. With no detailed clarification on the relationship between these different data classification systems (see item (4) below), it would be extremely burdensome for FIs to align these requirements into one integrated data categorisation/classification mechanism that can be applied in practice.

If the PBOC is firmly of the view that the introduction of a new classification system is required for FIs in the PRC, considering the large scale of data typically processed by an FI, we suggest that the PBOC limits the classification methodology to one uniform set of criteria, ideally the three different types of data in line with the upper-level principles of the PRC Data Security Law ("**DSL**"), and clarify the definitions of each of these type of data. Differing levels of data security can then be readily understood by personnel within FIs and their customers and other stakeholders, and applied and relied on accordingly. For example, regarding the data inventory requirement from a data categorisation perspective, Article 7 states that data processors must "identify whether each data item is personal information and its data source (production, operation, processing, external collection, etc.), the list of information systems where data item is stored and the types of business application". Having such granular requirements for one sub-set of "general data" would already impose significant compliance burden on FIs. Indeed, we further propose that these requirements should be prescribed as recommended standards instead of mandatory requirements (or, at least, that an FI can choose to adopt only one method of classification from various options presented by the Draft Measures), thereby releasing potentially heavy operational burden for FIs to which such requirements might be less relevant.

Further to the recommendation above, Articles 5, 7 and 9 of the Draft Measures set out scenarios where industry standards must be referred to by FIs in their compliance practices. Our understanding, however, is that the industry standards are not intended to be mandatory because they are not suitable for all organisations in all circumstances. We recommend that PBOC clarifies under the Draft Measures whether compliance with these industry standards is mandatory or they only serve as non-binding guidance for in-scope organisations, such that the market dictates adoption levels.

Moreover, as data classification by FIs is usually an automated process (given that the volume of data that FIs handle), it would not be necessary or realistic to approve the results of their data classification activities, as proposed in Article 6. We recommend that the PBoC removes any requirement for these results to be approved on a granular basis, replacing this (if at all) with a requirement only to approve the methodology of data classification.

(2) Classification standards of three levels require further clarification

Article 8 of the Draft Measures states that data must be classified into three levels based on its precision, scale and degree of impact on national security: general data, important data and core data.

The term "precision" did not appear in previous standards of data classification and protection (i.e. *Financial data security – guidelines for data security classification (金融数据安全 数据安全分级指南)*), while we understand a similar term, the level of "accuracy", is used and covered under the level of "integrity" of data. We recommend retaining this reference to the level of integrity to align with the current data classification practice. However, if the level of "precision" is different from the level of "accuracy", we recommend PBOC clarifying the definition of precision.

Moreover, for data to be so classified, it is not clear whether:

(a) the PBOC's expectation is that classification is undertaken at a certain milestone (at which, for example, a complete review can be undertaken) or this must be an ongoing assessment – and, if so, at what frequency – given that these factors (in particular, precision and scale) will change constantly;

(b) whether it includes structured or unstructured data; and

(c) organisations must determine themselves the relevant influence of "precision" and "scale" to the overall "impact on national security" of data, or PBOC will provide further guidance on this.

We understand that some of these factors have been explored before in draft standards such as the Information Security Technology – Rules for Identification of Important Data.

(3) Classification of data based on degree of harm should be aligned with existing standards

Article 4.2 of the *Personal Financial Information Protection Specifications (《个人金融信息保护技术规范 (JR/T0171-2020)》)* classifies personal financial information by reference to three levels (C1, C2 and C3) based on the degree of sensitivity to harm attaching to the information. If a system of classification referenced to sensitivity is to be retained, to align with this standard, we recommend that the Draft Measures classifies data based on:

(a) three levels of sensitivity instead of five; or

(b) if five levels are to be used, the upper two levels could have voluntarily application depending on an organisation's own data environment and internal policies. If five levels are used, we also recommend PBOC clarifying whether the five levels are identical to the five levels of sensitivity in the *Financial data security – guidelines for data security classification* – without a clear classification criterion, it is difficult for FIs to evaluate the exact operational requirements for compliance, especially where controls must be implemented on low sensitivity data (i.e., "level 2" data).

One rationale for recommending that only three levels of sensitivity are applied as a

mandatory obligation is that five levels are particularly impractical for FIs with no retail banking business. We recommend that PBOC leaves more flexibility for these FIs to only apply three levels of data classification in the Draft Measures (i.e., by reference to general, important and core data), so that these FIs can adopt their existing data classification approach to efficiently comply with the Draft Measures.

(4) Relationship between different data classification systems needs clarification

Data classification systems based on sensitivity, availability and impact on national security may overlap. In-scope data processors would then have uncertainty as to which protective measures under the Draft Measures to apply to a particular data set. For example, is it acceptable for core data to be rated as "level 1" in respect of sensitivity?

Moreover, we understand that the criteria for each classification system seeks to address different risks, which may be achievable through a simpler system in order to reduce operational burden for FIs and the practical challenge for PBOC of consistent supervision and enforcement. For example, all important data could be considered by default as "level 4" in respect of sensitivity.

We recommend that PBOC further considers how the multiple systems work together for any one FI and:

(a) ideally, dispenses with the need for a mandatory classification system specific to these business lines; or

(b) if some form of system needs to be retained, greatly simplifies the classification systems and clarifies which existing industry standards (if any) are an appropriate reference.

(5) Determination of important data remains unclear

Article 5 of the Draft Measures states that PBOC is responsible for organising and formulating relevant industry standards for data classification by category and grade, guiding data processors to carry out data classification by categories and grades, coordinating and determining the specific directory of important data and implementing dynamic management. Article 8 further states that data processors must accurately identify and determine whether any data stored in their information systems is important data or core data, and a filing needs to be made to PBOC regarding this determination.

A concept of "important data" was introduced in the PRC Cybersecurity Law back in 2017 and the apparent attachment of data localisation and other stricter obligations (compared to general data) has inhibited some FIs – in extreme cases – from investing or expanding in the Chinese market because of the perceived sensitivity linked to financial services. We urge PBOC to issue any such catalogue or directory of important data (and, if relevant, core data, assuming these are the same concepts introduced together in Article 21 of the DSL) to allow FIs and other in-scope organisations to understand what this constitutes in the financial services industry.

3. Coordination with higher-level laws and existing regulations from PBOC, CSRC, NAFR and other authorities

(1) Facilitating the holistic management of data

Depending on specific type and business of an FI, its data management may be under the supervision of one or more of financial regulators, such as PBOC, NAFR, CSRC and/or

other authorities. The requirements of different regulators may overlap or even in conflict. For example, there are already existing data classification rules or standards released by the CSRC and other financial regulators, which set out different criteria of data classification with those in the Draft Measures. It would be difficult for FIs to observe different sets of rules if these regulators do not coordinate among themselves in the area of supervision, i.e., data management in this case.

Specifically, the Draft Measures set a minimum data record retention period of three years for different types of data in Articles 17, 18, 20, 23, 24, 26, 28, 31, 39 and 45, while the existing NFRA, CSRC and PBOC regulation on *Administrative Measures for the Identification of Financial Institution Clients and the Preservation of Clients' Identities and Transaction Records* (*《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》*, see Article 29) requires FIs to keep clients' identities and their transaction records for at least five years. We appreciate PBOC's proposal for shorter periods for record retention but, for this to be meaningful, we request that PBOC seeks agreement with the other relevant authorities for a similar reduction under the other rules. If not achieved, a disparity among rules can lead to confusion for internal compliance functions of FIs and from an audit perspective.

We, therefore, recommend that PBOC coordinates with the other financial regulators as much as possible and:

(a) ideally, dispenses with the need for the Draft Measures entirely given existing laws and regulations published by it and other regulators; or

(b) if the Draft Measures are to be retained, align the PBOC's requirements under the Draft Measures with those under existing laws and regulations published by it and other regulators.

Alignment with existing rules would not only be critical for FIs' compliance with multiple rules released by different regulators, but also facilitate the stability and continuity of their business, such as the cross-border RMB business – namely existing business models that are beneficial to the wider Chinese economy domestically, and in some cases internationally, would not be impeded by conflicting regulation nor would a new business or management mechanism be needed in complex financial transactions if new rules are formulated to align with existing requirements. In particularly in respect of cross-border RMB transactions, we request that PBOC provides more clarity on how the new requirements under the Draft Measures would be applied to foreign entities given that the adoption of same standards for cross-border transactions as domestic transactions could be expected to have detriment impact on the internationalisation of the RMB due to the confusion and concern of foreign FIs using RMB under such rules.

(2) Technical requirements should be consistent

For technical-related requirements imposed under the Draft Measures, we recommend PBOC to align with the DSL, which requires data processors to leverage the existing "multi-level protection scheme" ("**MLPS**") for their data protection obligations. FIs have been implementing MLPS to protect systems and data, and new competing regimes, if not coordinated, could create confusion, fragmentation and inconsistencies that negatively impact data security and cybersecurity.

For areas that NAFR and CSRC already have existing technical requirements such as on recovery point objective and data restoration test/validation, we recommend PBOC to align with existing NAFR and CSRC requirements. For example, on data recovery, the *Measures*

for the Administration of Network and Information Security in the Securities and Futures Industry (2023) (《证券期货业网络和信息安全管理办法》) released by the CSRC require FIs to conduct quarterly back-up data verification for important information systems. PBOC's recommended industry standard for MLPS, the *Implementation guidelines for classified protection of cybersecurity of financial industry – Part 2: Basic requirements (2020) (《金融行业网络安全等级保护实施指引 第2部分：基本要求》),* also states that MLPS Level III applications should conduct quarterly back-up data verification.

However, in Article 33(4) of the Draft Measures, FIs are required to verify the back-up data everyday if the system's recovery point objective is shorter than 10 minutes. This is inconsistent with existing requirements and standard and will be very challenging for FIs to follow in practice. If a change of current industry practice is absolutely needed, we recommend PBOC to coordinate with NAFR and CSRC to ensure alignment and consistency between the existing rules and any supplementary requirements to be proposed by PBOC.

(3) Financial industry standards

Various references are made in the Draft Standards to financial industry standards. It is not clear, however, whether these standards are those released by the Standardisation Administration of China and/or the State Administration for Market Regulation, rather than those released by private organisations.

We recommend that this is clarified definitively in any revised version of the Draft Measures by reference to industry standards being those issued by national bodies such as Standardisation Administration of China or State Administration for Market Regulation.

4. Embedding risk-based approach in practice of FIs to self-regulate data security protection to add operational flexibility

The Draft Measures require prescriptive encryption for data classified as "level 3" and "level 4" without taking into consideration the actual control environment.

We recommend that PBOC takes a risk-based approach to data security and allows FIs to design controls based on risk considerations such as the impact level of data loss/damage and the possibility of an incident occurring. For example, it is already industry practice that:

(a) if sensitive data is stored in an application which is not client-facing or internet-facing and with proper perimeter security control, data encryption at rest may not be necessary given the possibility of an incident occurring that could cause data loss or compromise is low; and

(b) volume thresholds will be set so that low volumes of highly sensitive data can have comparatively lighter encryption controls.

Compared with most organisations, FIs are mature organisations in a highly regulated industry, and have extensive processes for securing data and respecting national security considerations. Given this, we recommend that PBOC allows self-regulation of data security to increase operational flexibility and, as a result, innovation and efficiencies to the benefit of customers.

5. Grace period to provide sufficient time for FIs' implementation of the Draft

Measures

The Draft Measures will, once launched, have a material impact on the relevant FIs and other in-scope data processors.

We urge PBOC to provide a grace period for compliance with the Draft Measures' requirements so that the relevant FIs and data processors have sufficient time to adjust their data processing practices. By reference to important international precedent, we recommend PBOC to follow the two-year grace period set for the launch of the European Union's General Data Protection Regulation.

6. Data Security Management Principle

Examining the proposed principle of "who manages business, who manages business data, and who manages data security", there are many technical and organisational measures that cannot be conducted by every business data owner in respect of data security management. Indeed, in our experience, data security management requires coordinated effort from various functions, including the information security team and operations department.

We recommend that the PBOC revisits this principle and proposes an alternate methodology for managing data security which is more pragmatic and recognises that effective data security management can only be achieved with the combined effort of all stakeholders in a business and cannot be managed solely by the business data owner. By referring to so-called "Big Data Management Regulations" issued by various local governments in the PRC, we recommend that PBOC adopt a similar principle that expands the scope of personnel to which responsibility attaches from solely the data owner to any data user – namely, "data security responsibilities are determined in accordance with the principles of who owns is responsible, who holds is responsible, who manages is responsible, who uses is responsible, who collects is responsible".

7. Other specific terms to be further clarified

Certain articles in the Draft Measures set out terms that are unclear and they generally invoke concern among our members because of this uncertainty. They include:

(a) Article 4 – The impact of the "national data security work coordination mechanism" on the scope and way the PBOC will supervise FIs' data security management is unclear. For example, it is not explained whether the policy intention is only to supervise core data management activities. We recommend that PBOC clarifies the extent of the change to the PBOC's top-level supervision in this respect to assist in overall transparency.

(b) Article 12 – FIs are expected under this proposed article to define the responsibilities of internal departments for data security management. In practice, the head of a business line or a corporate function usually owns the relevant data. We recommend that PBOC provides further guidance on how it expects the delegation of responsibility to each business unit, and the expected role and number of the data security management staff in each unit, or otherwise clarify that this is to be determined by FIs.

(c) Article13 – The proposal under this article suggests that data processing activities carried out jointly – whether domestic or cross-border – must maintain equal or higher levels of security protection management and technical measures. Firstly, we recommend that the

PBOC clarifies the scope of "joint data processing" because it is unclear what this is and whether it applies in the case that the other party is outside of the PRC. Secondly, we recommend (depending on the nature of the relationship envisaged by the PBOC) that PBOC clarifies whether the relevant security protection management and technical measures can be set out in service level agreements between parties. Thirdly, in light of the State Council's release of the *Opinions on Further Optimising the Foreign Investment Environment and Intensifying Efforts to Attract Foreign Investments*, which, among others, propose implementation of security management mechanisms that facilitate freer cross-border data flows for foreign-invested companies in China, we believe that the Draft Measures should not be drafted to increase the burden on cross-border transfers but rather they could introduce more liberalisation measures.

(d) Article 17 – Sub-article (3) of this article clarifies that when FIs collect data indirectly from individuals, the FIs should require the data provider to obtain valid consent from the individual and, for non-written consent, the data provider should be required to issue explanatory materials on the source of the data. These steps should then allow the FI to evaluate the legality and authenticity of the relevant consent. We recommend that the PBOC clarify that the compliance requirements under this article for the indirect collection of data can be applied to other indirect collection/processing activities of FIs in respect of data. More widely, while this sub-article would only seem relevant to the collection of personal information, the text of the whole of Article 17 is not clear as to whether it applies to personal information or all types of data. We recommend that the PBOC clarifies its intention here by amending Article 17 accordingly and to exclude certain scenarios. For example, when conducting corporate banking businesses, FIs need the information of authorised persons, traders, directors, and senior management of corporate clients. Such information is provided by the corporate to the FIs, and it is one of the scenarios where "data is not collected directly from individuals or organisations". In this case, the corporate client, as an independent data processor, has the legal obligation to ensure legality and other compliance aspects are met when processing the personal data that it collects and processes but it is possible for these clients to process the data under legal bases other than consent. As such, the Draft Measures should more explicitly exclude certain activities and not impose additional obligations on FIs (as the data recipients) such as obtaining unnecessary consents or reviewing the lawfulness of the data processing where other laws do not require these steps.

(e) Article 18 – "terminal device or removable media": We recommend that the Draft Measures define the term "terminal device or removable media". In particular, are tablets, desktop and laptop computers considered to be terminal devices? Further, we request that, if corporate devices such as tablets, desktops and laptops are be included in the definition of "terminal devices", these be allowed to process or temporarily store "level 3" data or above for as long as security controls (such as hard disk encryption) are in place.

(f) Article 20 – "in a proper manner": We recommend that the meaning of the term "in a proper manner" in the second paragraph of this article is clarified. In particular, is there any difference between the term "in a proper manner" in this article and the term "expressly stated" in Articles 17(1) and 37(2)?

(g) Article 21 – We are of the view that sharing of de-identified personal information in a secure environment carries no practical risk to individuals. As such, we recommend that the Draft Measures confirm that de-identified personal information is excluded from the calculation of the data volumes referenced in the phrases "provision of personal information abroad by data processors who process personal information of more than

1 million persons" and "provision of personal information abroad of more than 100,000 persons from January 1st of last year" under Article 4 of the Security Assessment Measures for Outbound Data Transfer.

(h) Article 22 – "instant messaging tools": The Draft Measures state that "instant messaging tools" cannot be used to exchange or transfer data items of "Level 3" or above unless the data processors clarify the specific scenarios, provide necessity analysis and implement risk prevention measures for each scenario. However, the *Notice on Regulating the Use of Instant Messaging Tools for Interbank Market Transactions (《关于规范银行间市场交易即时通讯工具使用有关事项的通知（2021）》)* released by the National Association of Financial Market Institutional Investors ("**NAFMII**") states that transactional instant messaging tools with functions such as real-name authentication, access right management, information traces, and record keeping can be regarded as approved standard business operations. We recommend that PBOC clarifies if the risk prevention measures in Article 22 of the Draft Measures are met by the above NAFMII requirements. In addition, we recommend that PBOC distinguishes between personal and enterprise versions of instant messaging tools, as the enterprise version of WeChat has been deemed to meet the NAFMII requirements.

(i) Article 24 – "Office for National Data Security Coordination Mechanism": We recommend it is clarified what information is needed, what procedure applies and what other requirements exist, when submitting a report to the Office for National Data Security Coordination Mechanism for approval in the second paragraph of this article.

(j) Article 27 – "approval": FIs are under regulatory obligations to provide data to overseas regulators (both home regulators and where the FIs may have significant operations). In some cases, failure to provide such information to foreign regulators as part of mandatory regulatory reporting could breach the requirements that these FIs must meet in order to be permitted to carry on regulated activities in those other markets. Among other things, foreign FIs may be required to have the ability and resources to measure, monitor and manage risk on a consolidated basis. Accordingly, it will be important to have a clear understanding and as much certainty as possible from PBOC as to how the approval process will operate and what criteria PBOC will take into account in deciding whether it will approve these mandatory data reporting obligations. We recommend that the procedure for seeking approval from the PBOC is set out under the Draft Measures or other guidance, where there is a genuine need to provide data to a foreign financial agency. We suggest that it is also clarified if approval is required from any regulatory authorities other than PBOC. We also recommend that the scope of the restriction on cross-border data transfers under this article is narrowed to data under the supervision of the PBOC, in alignment with the scope of similar restrictions under Article 177 of the Securities Law (2019 revised) and Article 124 of the Futures & Derivatives Law.

(k) Article 31 – This article proposes that data processors must establish a unified log specification and specify the information required for tracing data processing activities in these logs. We recommend that the requirements for data processing logs be managed according to the sensitivity level of data and that log records are not mandatory for extremely low-sensitivity data.

(l) Article 33 – "more than one million people": We recommend that the basis is clarified for calculating one million persons in the "important data or personal information of more than one million people" stipulated in the second paragraph of this article? In particular, is it required to take multiple pieces of information of the same person into account?

Moreover, we recommend setting criteria that exclude personal information from this calculation where the information is processed for the purpose of scenarios where a cross-border transfer is intrinsically required, such as payment instruction fulfillment and/or executing the related products.

(m) Article 36 – "security protection measures": We recommend that the security protection measures described in the first paragraph are clarified as being optional or mandatory. Furthermore, in the current form of the Draft Measures, it is unclear whether it necessary to fulfil all requirements of the "dedicated lines, virtual private networks, and secure communication protocols" or it is sufficient to fulfil one of them.

(n) Article 37 – "centralised technical platform for continuous data provision activities": We recommend that the criteria / qualifications when determining the "centralised technical platform for continuous data provision activities" in the first paragraph of this article are stipulated.

(o) Article 39 – "in a timely manner": We recommend that it is stated whether a specific deadline applies for "destroyed in a timely manner" in the first paragraph of this article.

(p) Article 40 – "effective measures": We recommend that it is clarified whether the risk monitoring measures referred to in this article are optional or mandatory.

(q) Article 43 – "entrusted testing agency": It is not clear whether there are any qualification requirements for the entrusted testing agency or other requirements related to selection. We recommend that the PBOC issues guidance for this. We also suggest that further guidance on the methodology and detailed requirements on the risk assessment should be released.

(r) Article 44 – "data security audits": Given FIs already undertaken audits, we recommend that it is clarified if the "data security audits" can be covered by other specialised audits or comprehensive risk audits.

(s) Article 47 – "emergency drills for data security incidents": Similarly, FIs already undertake "emergency drills for data security incidents". We recommend that it is clarified whether the drills mentioned in the second paragraph of this article can be covered by other emergency drills or at the institution-wide level.

Next steps

As we understand the importance of such regulation for the business and economic environment in the PRC, we would be pleased to engage in further discussions with the PBOC. ASIFMA and our members are ready to provide further details and to engage in constructive dialogue on the proposed Draft Measures.

Should you have any questions in relation to this letter or would like to obtain further industry input, please contact Diana Parusheva, Executive Director at ASIFMA, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.

In the meantime, to facilitate dialogue, we will also share a copy of our submission with the CSRC and NAFR, given the potential overlapping areas of regulation.

This submission was prepared with the assistance of the law firm Zhao Sheng Linklaters (FTZ) Joint Operations Office, based on feedback from the wider ASIFMA membership.

Yours faithfully

Diana Parusheva-Lowery
Head of Public Policy and Sustainable Finance
Asia Securities Industry and Financial Markets Association (ASIFMA)
F: +852 9822 2340
DParusheva@asifma.org
www.asifma.org