28 November 2021

2021 年 11 月 28 日

Cyberspace Administration of China,

No. 11, Che Gong Zhuang Da Jie, Xicheng Qu

Beijing Shi, People's Republic of China

国家互联网信息办公室

北京市西城区车公庄大街 11 号

[shujuju@cac.gov.cn]

CC: People's Bank of China; China Securities Regulatory Commission; China Banking and Insurance Regulatory Commission

抄送：中国人民银行；中国证券监督管理委员会；中国银行保险监督管理委员会

Dear Sir/Madam:
尊敬的先生/女士:

RE: The Consultation Draft of the Measures for the Security Assessment of Data Outbound Transfer
关于：《数据出境安全评估办法（征求意见稿）》

The Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] welcomes the opportunity provided by the Cyberspace Administration of China (the "**CAC**") to submit comments and suggestions on the draft Measures for the Security Assessment of Data Outbound Transfer (**《数据出境安全评估办法》**) (the "**Measures**")[2].
亚洲证券业和金融市场协会(**"ASIFMA"**、**"本协会"**或**"我们"**)很荣幸有机会就国家互联网信息办公室（**"贵办公室"**）发布的《数据出境安全评估办法（征求意见稿）》（**"《评估办法》"**）提出意见和建议。

ASIFMA appreciates the CAC's efforts to further develop the current rules and standards relating to cross-border transfers of data. We support the need to establish reasonable and proportionate mechanisms to safeguard data outbound transfer. Data is pivotal to the business of our members, and providing corresponding protection for appropriate data transfer while protecting data security is essential to the integrity of financial markets and customer, and business confidence more broadly.
ASIFMA 十分赞赏贵办公室为了进一步发展与数据跨境传输相关的现有规则和标准所作出的努力。我们明白建立合理及适当的数据出境安全评估机制的需要。数据是本协会成员开展业务经营的关键，在保护数据安全的同时对合理的数据传输提供相应保护，对于健全金融市场及稳定消费者和经营者信心也至关重要。

We have consulted our members and received responses. This letter sets out our views on the draft Measures, the practical difficulties financial institutions may face, and our recommendations. In this letter, we also seek clarification on the application of, and suggest amendments to, certain provisions of the draft Measures with the aim of striking a better balance between data security, privacy protection and the commercial use of data (including

[1] ASIFMA is an independent, regional trade association with over 150 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA provides insights on global best practices and standards to benefit the region. The mission of ASIFMA is to promote the development of liquid, deep and broad capital markets in Asia, which is fundamental to the region's economic growth. ASIFMA drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. The initiatives of ASIFMA 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.
ASIFMA 是一个独立的区域性行业协会，会员基础广泛，由银行、资产管理公司、律师事务所和市场基建服务供应商等 150 多家来自买方和卖方市场的领先金融机构和专业机构组成。ASIFMA 通过全球金融市场协会（GFMA）与美国的证券业与金融市场协会（SIFMA）及欧洲的金融市场协会（AFME）形成联盟，共同提供全球最佳行业实践及标准，为区域发展作贡献。ASIFMA 的使命是促进在亚洲建立发展一个流动性强并具有深度和广度的资本市场，这对于支持亚洲地区的经济增长是十分关键的。ASIFMA 通过汇聚集体力量和统一行业发声，围绕关键问题推动形成共识、提出解决方案建议并促成变革。ASIFMA 采取的努力包括与监管机构和交易所进行磋商、制定统一的行业标准、通过政策文件推动改善市场，并降低在地区内开展业务的成本。

[2] http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

information sharing), and achieving clearer compliance guidance for data processors. Unless otherwise specified, articles mentioned in this letter refer to the articles in the draft Measures.
我们已征求我们会员的意见并得到积极回应。本函件载列我们关于《评估办法》的意见、金融机构可能面临的实际困难以及我们的建议。在本函中，我们希望能明确《评估办法》中的部分条款的适用问题，并谨对部分条款提出修改建议，旨在更好地平衡数据安全、隐私保护和数据的商业运用（包括信息共享），并为数据处理者提供更清晰的合规指导。除另有说明外，本函件所称条款均指《评估办法》中的条款。

Overview of Feedback
反馈意见概述

We understand that the Measures seek to set out implementation details regarding security assessments that data processors are required to carry out under existing laws including the Cybersecurity Law ("**CSL**"), the Data Security Law ("**DSL**") and the Personal Information Protection Law ("**PIPL**").
我们理解，《评估办法》是根据《中华人民共和国网络安全法》（"**《网络安全法》**"）、《中华人民共和国数据安全法》（"**《数据安全法》**"）和《中华人民共和国个人信息保护法》（"**《个人信息保护法》**"）等现行法律对数据处理者在上述法律项下应当进行的数据安全评估所制定的实施细则。

Our members believe that integral to their capability to function resiliently and to the standards that their clients and parents demand is an ability to transfer data transnationally without undue impediment or administrative burden. In the view of our members, the CSL, DSL and PIPL already impose significant barriers to the free-flow of data which is beyond that experienced in other global financial centres.
我们的会员认为，对于维持经营能力以及满足客户和母公司所要求的标准而言，能够在没有不当障碍或行政负担的情况下进行数据的跨境传输是不可或缺的。在我们的会员看来，《网络安全法》、《数据安全法》和《个人信息保护法》已经对数据的自由流动设置了较大的障碍，与其他国际金融中心的做法有所偏离。

Data transfers facilitate fraud prevention, anti-money laundering, execution of cross-border business, the ability to effectively manage cyber threat, regulatory compliance and the exchange of knowledge and ideas that allows our members to add real value to Chinese consumers, enterprises and the Chinese economy as a whole.
数据传输有助于反欺诈、反洗钱及开展跨境业务，亦增强网络威胁管理能力、提高合规性并促进知识和思想的交流，从而使我们的会员能够从整体上为中国消费者、企业和整个中国经济提供正向价值。

Other global financial centres seek to support necessary cross-border data flow through internationally-recognized, practical mechanisms that do not require manual, time-consuming government reviews. Such mechanisms include Standard Contractual Clauses, Binding Corporate Rules and independent certification. We strongly recommend that the CAC align with global practice on cross-border data transfers.

其他国际金融中心均通过国际公认的切实可行的机制支持必要的跨境数据流动，该等机制无需政府耗费人力和时间进行审查。该等机制包括标准合同条款、约束性企业规则和独立认证。我们强烈建议贵办公室在跨境数据传输方面对标该等国际实践。

However, our members also understand that in certain circumstances, China may have unique requirements, including control of data deemed central to China's national security. In order to enable protection of such interests without stifling normal business operations, our members would respectfully urge the CAC to focus any government-led review of data export on well-defined categories of sensitive data. This focused approach will have dual benefits of supporting efficient business and better leveraging the CAC's limited and precious administrative resources.
与此同时，我们的会员也充分理解，中国可能针对某些场景适用特色化的要求，例如对与国家安全相关的数据进行严格管控。为了在不妨碍正常业务运营的情况下保护该等利益，我们的会员恳请贵办公室将由政府机关主导的数据出境审查的重点放在定义明确且相对敏感的数据类别之上。该等重点管理的方法能够促进商业效率，亦能让贵办公室更好地运用有限但宝贵的行政管理资源。

We note with particular concern that:
我们特别注意到：

- the Measures, to a certain degree, seek to broaden requirements under existing laws; and,
  《评估办法》在一定程度上加重了现有法律项下的要求；以及
- when introducing new requirements, leave certain areas open to interpretation without the clarity required for data processors to be secure in designing their compliance programs to align with the CAC's expectations.
  在推出该等新要求时，部分要求并不清晰、有待进一步的解释，这导致数据处理者在制定符合贵办公室期望的合规计划时欠缺明确指引。

Detailed Feedback
具体反馈意见

1. Distinction between "Security Assessment" and "Risk Self-Assessment"
"安全评估"和"风险自评估"的区别

We note that the Measures seek to articulate detail in relation to two separate types of assessment namely:
我们注意到，《评估办法》旨在阐明两种不同评估类型的具体要求，即：

- A "Security Assessment" – a State-conducted security assessment carried out by the CAC. This appears to refer to the security assessments required under Articles 38(1) and 40 of the PIPL and Article 37 of the CSL; and,
  "安全评估"——由贵办公室执行的国家安全评估。这似乎指的是《个人信息保护法》第 38 条第（一）项和第 40 条以及《网络安全法》第 37 条要求的安全评估；以及
- a "Risk Self-Assessment" – a data processor conducted self-assessment carried out by the organization wishing to export data. This appears to be a new requirement that does

not currently arise under the CSL, the DSL or the PIPL. Where a State-led Security Assessment is required, this Risk Self-Assessment is a preliminary step that the data processor must carry out and submission of the report detailing the results of this Risk Self-Assessment is required to submit for the State-led Security Assessment. In other circumstances where a State-led Security Assessment is not required, a Risk Self-Assessment seems to be the only step required prior to a cross-border data transmission being made.

"风险自评估"——由希望向境外提供数据的的数据处理者进行的自我评估。《网络安全法》、《数据安全法》或《个人信息保护法》项下似乎并没有该等规定。在需要国家安全评估的场景下，风险自评估是数据处理者必须执行的前置步骤，并且数据处理者在申报安全评估时需要就风险自评估结果提交详细说明。在不需要安全评估的其他情形下，风险自评估可能是进行跨境数据传输之前唯一需要的步骤。

For the purposes of these comments, we use these two terms as defined above.
为本函之目的，我们使用如上定义的两个术语。

2. Triggers for "Risk Self-Assessment" under Article 5
第 5 条项下"风险自评估"的触发条件

There are different interpretation for Article 5, literally the self-assessment referred to in Article 5 covers outbound transfer for all data, but Article 6 mentioned that Risk Self-Assessment is a preliminary step of Security Assessment that some market players tend to understand the self-assessment may cover only the data specified in Article 2. If a Risk Self-Assessment is required whenever any data processor provides any "data" abroad, this is a very onerous requirement, the scope of which goes far beyond the requirements seen to date under the CSL, DSL and PIPL. We would suggest that a more reasonable requirement may be that such Risk Self-Assessments need only be carried out in circumstances that a data export includes a type of data deemed sensitive under the CSL, DSL and PIPL, that being the data specified as triggering a Security Assessment under Article 2, namely: (i) personal information ("PI") which requires a Security Assessment under the CSL or PIPL and (ii) important data collected and generated through firms' business operations in China.

第 5 条可能存在不同解读，如果从字面上进行解读，风险自评估适用于所有数据出境的场景，而结合第 6 条的规定，因风险自评估是安全评估的前置程序，似乎风险自评估仅针对第 2 条中规定的数据。如果风险自评估适用于任何数据处理者向境外提供任何"数据"，这将是一个非常苛刻的要求，远超出了《网络安全法》、《数据安全法》和《个人信息保护法》中的要求。我们希望贵办公室能采用更合理的要求，例如只有在出境的数据中包括《网络安全法》、《数据安全法》和《个人信息保护法》中所规定的敏感的数据类型的情况下，才需要进行此种风险自评估，即第 2 条规定的触发安全评估的数据，分别为：(i)根据《网络安全法》或《个人信息保护法》需要进行安全评估的个人信息，以及(ii)在中国境内运营中收集和产生的重要数据。

3. Triggers for "Security Assessment" under Article 4
第 4 条下"安全评估"的触发因素

We note that Article 4 introduces a series of triggers for a Security Assessment that widen the existing requirements under the CSL, DSL and PIPL. We would respectfully suggest that the Measures should not broaden requirements under existing law.
我们注意到，第 4 条规定了一系列安全评估的触发因素，扩大了《网络安全法》、《数据安全法》和《个人信息保护法》的现有要求。我们谨此建议，《评估办法》不应扩大现有法律的要求。

Under the CSL (Article 37), critical information infrastructure ("**CII**") operators that gather or generate PI and important data during operations in China need to store PI and important data in China unless export is necessary, in which case, they are required to go through a Security Assessment. The PIPL (Article 38 and 403), repeats the CSL requirements of CII operators gathering and generating PI and also adds that data processors handling a certain amount of PI prescribed by the CAC also need to comply with the same requirements. The PIPL also states that for all other types of PI processors, Security Assessment is not mandatory prior to export, instead export is permitted subject to fulfilling one of four possible conditions (only one of which is a Security Assessment).
根据《网络安全法》（第 37 条），关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，则需要通过安全评估。《个人信息保护法》（第 38 条和第 40 条）也重申了《网络安全法》对收集和产生个人信息的关键信息基础设施运营者的要求，同时规定，处理的个人信息达到网信部门规

[3] **Article 38** Where it is truly necessary for a personal information processor to provide personal information to a party outside the People's Republic of China for business or other needs, the personal information processor shall satisfy one of the following conditions:
(1) passing the security assessment conducted by the cyberspace administration department of the State in accordance with Article 40 of this law;
(2) undergoing personal information protection certification conducted by a specialized agency in accordance with the requirements of the cyberspace administration department of the State; (3) concluding a contract with the overseas recipient in the standard form promulgated by the cyberspace administration department of the State to agree on the rights and obligations of both parties; and
(4) meeting the other conditions prescribed by laws, administrative regulations, or the cyberspace administration department of the State.
Where an international treaty or agreement concluded or acceded to by the People's Republic of China has provisions on the conditions for the provision of personal information to a party outside the People's Republic of China, such provisions may be followed.
The personal information processor shall take necessary measures to ensure the overseas recipient's personal information handling activities meet the personal information protection standards specified in this law.
第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：
（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；
（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；
（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；
（四）法律、行政法规或者国家网信部门规定的其他条件。
中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。
个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。
Article 40 Critical information infrastructure operators and personal information processors handling personal information that reaches the volume prescribed by the cyberspace administration department of the State shall store within the territory of the People's Republic of China the personal information collected and generated therein. Where it is truly necessary to provide such information to a party abroad, they shall pass the security assessment conducted by the cyberspace administration department of the State; where a law, administrative regulation or requirement of the cyberspace administration department of the State provides that the security assessment is not required, the provisions thereof shall be followed.
第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

定的一定数量的数据处理者也需要遵守同样的要求。《个人信息保护法》还规定，对于所有其他类型的个人信息处理者，在出境前不一定要进行安全评估，而是在满足四个可能的条件之一（其中仅有一个条件涉及安全评估）的情况下便允许出境。

While the Measures seek to introduce clarity on the PI volume thresholds (please see further comments on calculation of these below), these are not provided by existing laws and implementing regulations, and additionally, also subject additional categories of data processor to a mandatory Security Assessment.,
虽然《评估办法》试图对个人信息数量的门槛进行明确（请见下文关于数量计算的进一步阐释），但这些门槛在现行法规中并无统一标准。此外，《评估办法》还要求其他类别的数据处理者接受强制性安全评估。

Inconsistency of volume threshold definitions can be seen when comparing the Measures to the consultation draft of the Administrative Regulations on Network Data Security (《网络数据安全管理条例》(征求意见稿)) issued on November 14, 2021 (the "**Network Data Security Regulations**"). Under Article 37(2) of the Network Data Security Regulations the sole volume threshold-triggered basis for a Security Assessment is where a data processor processing PI of over 1 million persons exports PI, such threshold definition is consist with Article 40 of PIPL. While this aligns to Article 4(iii) of the Measures, there is no volume threshold equivalent to Article 4(iv) of the Measures set out in the Network Data Security Regulations. We would respectfully suggest that the Network Data Security Regulations and the Measures should align on triggers for a Security Assessment and that these should be set at a single trigger of that set out in Article 4(iii) of the Measures (with the trigger set out in Article 4(iv) of the Measures being removed).
如果将《评估办法》与 2021 年 11 月 14 日发布的《网络数据安全管理条例（征求意见稿）》（"**《数安条例》**"）进行比较，可以看出对数量门槛定义的不一致。根据《数安条例》第 37 条第（二）项，安全评估唯一的数量门槛的是处理一百万人以上个人信息的数据处理者向境外提供个人信息，这一规定亦与《个人信息保护法》第 40 条的规定相符。虽然《评估办法》第 4 条第（三）项也如此规定，但对于《评估办法》第 4 条第（四）项的数量门槛，《数安条例》并没有规定。我们建议，《数安条例》和《评估办法》应在安全评估的触发因素上保持一致，应仅规定《评估办法》第 4 条第（三）项下的数量门槛（《评估办法》第 4 条第（四）项规定的触发因素应当被删除）。

Lastly, under Article 4 of the Measures, additional categories of data processor are made subject to a mandatory Security Assessment namely when: (i) any data processor's data export includes any important data; and (ii) other circumstances arise in which the CAC specifies that a Security Assessment must be conducted. This is onerous for data processors. Given that the Article 31 of DSL has authorized CAC to formulate the implementing rules, and as CAC rolls out the Measures, we strongly recommend that the CAC limit the scope of data that will be subject to the CAC's security assessment to the extent necessary and practical.
最后，根据《评估办法》第 4 条，在以下情况下，其他类别的数据处理者必须接受强制性安全评估：(i)任何数据处理者出境数据中包含任何重要数据；以及(ii)出现国家网信部门规定的其他需要申报数据出境安全评估的情形。这对于数据处理者而言太过繁重。既然《数据安全法》第

31 条授权贵办公室制定相关政策，且贵办公室将正式发布《评估办法》，我们强烈建议贵办公室在必要和可行的范围内限制需接受安全评估的情形。

4. Definition of "Important Data"
"重要数据"的定义

Article 4(ii) requires that outbound transfer of important data is subject to security assessment. However, we note that the definition and scope of "important data" is yet to be definitively clarified. While we note that the Standardization Administration of China issued the consultation draft of Information Security Technology - Guidelines for Identifying Important Data in September 2021 and that the CAC Network Data Security Regulations also set out a criteria and mechanism for identifying "important data", we remain unclear on how "important data" will be identified within the financial services sector, or if indeed financial services firms will be deemed to generate or process important data. In particular, we note that financial business/activity related information is not specifically referred to as "important data" in the aforementioned September national standards (draft). We also remain unclear as to whether the Measures apply when an institution collects or is entrusted with the Important Data generated by a third party. For example, whether a financial institution would need to pass a Security Assessment prior to transferring IPO due diligence to an offshore affiliate even where the entity to whom the due diligence relates is already under an obligation to submit to and pass a Security Assessment prior to transfer of the data to a financial institution.
第 4 条第（二）款要求重要数据的跨境传输必须经过安全评估。然而，"重要数据"的定义和范围尚未明确。我们注意到，全国信息安全标准化技术委员会于 2021 年 9 月发布了《信息安全技术 重要数据识别指南》征求意见稿，贵办公室发布的《数安条例》也规定了识别"重要数据"的标准和机制，但我们仍不清楚在金融服务行业内如何识别重要数据，或者金融机构等金融服务提供者是否会被视为产生或处理重要数据的数据处理者。特别地，我们注意到，上述 9 月的《重要数据识别指南》征求意见稿中未将金融业务或活动相关信息列为重要数据。我们也还不清楚当机构收集第三方生成的重要数据或接受第三方对重要数据的委托处理时，《评估办法》这一要求是否适用。例如，金融机构是否需要在向境外关联方转让 IPO 尽职调查报告之前通过安全评估，即使尽职调查所涉及的实体已经有义务在向金融机构转让数据之前申报并通过安全评估。

We strongly recommend that to the extent financial services firms are deemed to generate or process "important data", that the categories of data which are thus deemed for financial institutions be narrowly limited to a (currently unpublished) catalogue of specifically articulated "important data".
我们强烈建议，若金融机构等金融服务者被视为生成或处理"重要数据"的数据处理者，金融机构的重要数据类别应严格限制在明确规定（但目前尚未公布）的"重要数据"目录。

We further suggest that strict compliance with Article 4(ii) should be waived in advance of the catalogue of "important data" applicable to financial institutions being published on the basis that categorization of important data by financial institutions is not possible without clear guidance. In addition, Article 4 (ii) provides that all the "important data" to be transferred outbound will be subject to security assessment, it would be extremely onerous and challenging for data processors. It is not practical to request the data processors to conduct

security assessment in regard of every outbound email containing "important data" during their day-to-day business operation. Thus, we appreciate if CAC could set a reasonable amount threshold for the important data, or to provide exemption accordingly.
我们进一步建议，在公布适用于金融机构的"重要数据"目录之前，第 4 条第（二）款的要求应被暂时豁免，因为如果没有明确的指导，金融机构无法对数据进行清晰分类并识别重要数据。此外，第 4 条第（二）项规定，所有出境的"重要数据"都将接受安全评估，这对数据处理者来说将是极其繁重和具有挑战性的，要求数据处理者在其日常业务运营期间对每封包含"重要数据"的出境电子邮件进行安全评估是不切实际的。因此，我们希望贵办公室能够为重要数据触发安全评估设定合理的数量门槛，或者提供相应的豁免。

5. Calculation of PI Volume Thresholds
个人信息数量门槛的计算

Article 4(iii) provides clarity on the PI volume processing thresholds referred to under Article 40 of the PIPL, and Article 4 (iv) provides similar volume threshold. We would request that the CAC clarify how the volume thresholds are calculated, and the timeframe over which such calculation should be made.
第 4 条第（三）项明确了《个人信息保护法》第 40 条所述的个人信息"达到国家网信部门规定数量"，第（四）项也明确了类似标准。我们希望贵办公室能够告知该等数量是如何计算的，以及什么时间范围内处理的个人信息应当被计算在内。

When considering the appropriate clarifications to provide on these points, we would suggest that:
在考虑合理地解释这些疑问之时，我们有如下建议：

- Carve-outs are made from the volume threshold calculations including:
  如下个人信息不应计算在规定的数量门槛内：
  - PI relating to individuals who are not Chinese citizens;
    非中国公民的个人信息；
  - PI relating to individual representatives of institutional clients (e.g. beneficial owners, directors, staff and representatives);
    机构客户的个人代表（如受益人、董事、员工合代表）的个人信息；
  - Intra-group transfers (including for human resources management).
    在集团内部转移的个人信息（包括为了人力资源管理而进行的）；
- Where it is necessary to transfer the same data back and forth in order to provide a service, that this is only viewed as one transfer as opposed to each transfer ex-China of the same data set constituting a new and distinct transfer;
  为了提供一项服务而必须来回传输相同的数据时，应当仅被视为一次传输，而相同数据集向中国境外的每次传输不应被视为是新的或不同的传输；
- The accumulated number of transfers refers to a number within a given period (e.g. one year) after which the cumulative count shall be reset instead of the count accruing over all time;
  累计传输的数据量应当是给定期间（如一年）内的累计，在此之后，应重新计算数量，而不是没有时间限制的持续累积；

- the commencement date for such calculation be specified, and in particular, whether the Measures have retroactive effect. So, for example, whether the date for calculation of PI volume runs for the date of incorporation of the entity or the effective date of the Measures and, whether once the volume threshold is exceeded, the data processor needs to submit all PI transfers for Security Assessment (including recurrent routine transfers) or only those occurring after the point in time at which the threshold is exceeded.
  明确计算的开始日期，尤其是明确《评估办法》是否具有追溯力。例如，计算个人信息数量的开始日期是否为数据处理实体成立之日或《评估办法》生效之日，以及一旦达到数量门槛，数据处理者是否需要提交自计算开始日后所有个人信息进行安全评估（包括经常性常规传输）或仅在达到数量的时间点之后传输的个人信息才需要进行安全评估。

6. Definition of "Sensitive Personal Information" under Article 4(iv)
第 4 条第（四）款"敏感个人信息"的定义

We would be grateful if the CAC could clarify whether the definition of "sensitive Personal Information" under Article 4(iv) has the same meaning as that under Article 28 of PIPL or Appendix B of Information security technology — Personal information security specification. In particular, we seek clarification as to whether any financial account information will be deemed as sensitive PI (or such information is only deemed as sensitive PI if, once leaked or illegally used, it may easily cause harm to the dignity of natural persons or harm to personal or property security).
我们恳请贵办公室能够澄清第 4 条第（四）款项下"敏感个人信息"与《个人信息保护法》第 28 条或《信息安全技术 个人信息安全规范》附录 B 规定的含义相同。特别地，请进一步说明是否所有金融账户信息均将被视为敏感个人信息；抑或是此类信息仅在一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害时，才被视为敏感个人信息）。

7. Definition of "outbound data transfer"
"数据出境"的定义

The definition of "outbound data transfer" is not specified. We recommend that the CAC may consider providing examples of which situations would be regarded as "data outbound transfer" and subject to the Measures. For instance, whether it covers the scenario where an offshore entity has access to view (but is not entitled to copy or maintain a copy of) the data located in an onshore data center.
"数据出境"的定义并不明确。我们建议贵办公室可以通过举例的方式，说明哪些情况会被视为"数据出境"并适用《评估办法》。例如，它是否涵盖境外实体可以查看（但无权复制或保存副本）位于境内数据中心的数据的情况。

We understand that the transfer of data to the Hong Kong Special Administrative Region, the Macau Special Administrative Region and Taiwan will be deemed as an outbound data transfer and thus regulated by the Measures. We appreciate if CAC could confirm this or further advise on it.

我们理解向香港特别行政区、澳门特别行政区和台湾地区传输数据亦将被视为数据出境，并因此适用《评估办法》。我们希望贵办公室能确认这一点，或者提供进一步的建议。

8. Authorities in charge of Security Assessment
负责安全评估的部门

1) CAC vs. financial regulator
网信部门 vs.金融监管机构

We would request further clarity on the authorities practically in charge of administering Security assessments. Article 10 provides that the provincial CAC may be involved in conducting Security Assessments as well as industry authorities. While we welcome and encourage the CAC to work closely and jointly with financial regulators in outbound data transfer related matters, we would also like to highlight that financial regulators have several existing requirements on cross-border data transfer that financial institutions need to observe and perform. Those requirements range from data protection, anti-money laundering and other personal information related obligations. Therefore, to the extent the relevant data transmission has been reviewed and endorsed by the financial regulators, we suggest that no duplicative reporting/application to the CAC is also required. We would request that the CAC and the financial regulators work together in formulating mutually recognized framework/standards and sharing information.
我们希望贵办公室就负责安全评估的主管部门进行澄清。根据当前第 10 条规定，省级网信部门与行业主管部门均将参与安全评估。我们欢迎并鼓励网信部门与金融监管机构在境外数据传输相关事宜上密切合作，但我们也想强调，金融监管部门在跨境数据传输方面已有金融机构需要遵守和执行的相关现行要求。这些要求包括数据保护、反洗钱和其他个人信息相关义务。因此，我们建议，如果相关数据传输已被金融监管机构审查和认可，则无需重复向网信部门进行报告或申请。网信部门和金融监管机构可以共同制定相互认可的框架及标准并分享信息。

We also consider it beneficial to regulators and industry players if security assessment on financial institutions is conducted / organized by financial regulators within the framework established together with the CAC (as mentioned above).
如果对金融机构的安全评估由金融监管机构在与网信部门共同建立的框架内开展（如上所述），我们相信这对监管机构和金融行业参与者都是有益的。

In addition, as we understand that the Measures will not be applicable to offshore data processors, so neither the CAC nor the financial regulators will enjoy any regulatory power to offshore data processors in regard of data cross-border transfer.
此外，我们理解《评估办法》不适用于境外数据处理机构，因此，我们希望贵办公室可以确认网信部门和金融监管机构在数据跨境传输方面均不对境外数据处理机构享有任何监管权力。

2) Special professional agencies
专门机构

We suggest the CAC clarify what “special professional agencies” in Article 10 refer to.

我们建议网信部门明确第 10 条中的“专门机构”的含义。

9. Security Assessment Application Documents
安全评估申请材料

1) Sample/template application documents
申请材料的样板/模板

Article 6 provides the requirements on relevant application documents for security assessment. In practice, it would ease the preparation and review of such application documents if the CAC could provide application templates for financial institutions to use as reference (without taking out the liberty of the applicant in preparing documents in other format which equally address the regulatory concerns as stated in the Measures). It will also be helpful if the CAC could clarify the scope of “other materials necessary for security assessment work” under Article 6(iv).
第 6 条规定了安全评估的相关申请材料的要求。在实践中，如果贵办公室能够提供申请模板供金融机构参考（该等模板并非强制适用或剥夺申请人以其他格式准备同等效果材料的自由），将便于申请材料的准备和审查。如果贵办公室能够进一步明确第 6 条第（四）项规定的“安全评估工作需要的其他材料 ”的范围，将会很有帮助。

2) Submission of contract with data recipients
与信息接收方订立的合同

Article 6(iii) requires the submission of the agreements between the data processors and the offshore recipients. We recommend removing Article 6(iii) as risk self-assessment (under Article 5(vi) and Article 6(ii)) already takes into account of data transfer related responsibilities and duties under the agreements. The requirement to submit the agreements between the data processors and the offshore recipients will call for far too much administration for both financial institutions and the CAC itself, given the need to extract each agreement with the offshore recipients, translate them into Chinese and piece them into a structured form that the CAC can process.
《评估办法》第 6 条第（三）项要求申报数据出境安全评估时应当提交数据处理者与境外接收方订立的合同。由于第 5 条第（六）项和第 6 条第（二）项规定的风险自评估已经考虑了该等合同项下与数据出境相关的责任和义务，我们建议删除这一要求。此外，该等规定使得境内数据处理者需要整理与每个境外接收方的协议、将合同条款翻译成中文并装订成便于贵办公室处理的形式，从而对数据处理者和贵办公室都带来繁杂的行政事务职责。

We suggest the CAC publish a template contract containing minimum requirements (but not intended to be a mandatory form) for the purpose of Article 9 so as to provide guidance to market players as well as ensuring minimum requirements are addressed in the contract.
我们建议贵办公室为《评估办法》第 9 条规定的数据处理者与境外接收方订立的合同提供一份规定最低要求的标准合同（但该等标准合同的形式并非强制适用），从而为数据处理者提供指导，并确保最低要求已经反映在标准合同中。

If the CAC intends to request more information about the contractual arrangement with data recipients, we advocate that firms should be allowed to provide summary of terms or redacted version, demonstrate appropriate controls, and leverage Standard Contractual Clause (SCC) for PI cross-border transfer.
若贵办公室依然希望了解与数据接收方的合同安排，我们建议允许数据处理者提供条款摘要或脱敏后的合同版本，展示其采取的适当的控制措施，或借鉴个人信息跨境传输的标准合同条款。

To speed up the assessment process with focused review, we recommend revising this requirement to submission of summary of data related key terms of the contract on a need-to-know basis instead of agreements themselves. Most of the commercial contracts have complex (and lengthy) provisions which do not necessarily directly relate to the matter on data security protection. The agreements may also be in English or other languages. It would be more efficient to provide a contract summary and focus on the data protection and data transfer related provisions in Chinese for the CAC to review.
为了推进安全审查的顺利进行，我们建议将这一要求修改为：基于了解的必要性，提交合同中与数据相关的关键条款摘要（而非合同本身）。大多数商业合同都有复杂且冗长的条款，这些条款不一定与数据安全保护直接相关，而且合同也可能是英语或其他语言的文本，提供侧重于数据保护和数据传输相关条款的中文合同摘要，亦有利于提高贵办公室的审查效率。

In addition, we also note that Article 38(iii) of the PIPL refers to a template agreement to be issued by the CAC for outbound data transfer and the concept of contractual protection as a means of facilitating cross-border data transfers is a key principle espoused here. We take the opportunity here to reiterate the importance of the CAC issuing the model clauses pointed to in the PIPL as one of the legitimate means for enabling cross border transfers of PI. We appreciate if the CAC can confirm that an agreement entered into containing the minimum requirements set out in such template would suffice the purpose of Article 9 (although a data processor may also use other form of agreement addressing the issues set forth in the template, such as the GDPR Standard Contractual Clauses).
我们还注意到，《个人信息保护法》第 38 条第一款第（三）项规定贵办公室将发布数据跨境传输标准合同。鉴于我们始终认为通过合同保护数据安全是促进数据跨境传输的重要原则之一，我们借此机会重申贵办公室发布《个人信息保护法》规定的标准合同作为允许跨境传输个人信息的合法手段之一的重要性。我们希望贵办公室能够明确根据标准合同规定的最低要求而制定并与境外数据接收方签订的协议足以满足《评估办法》第 9 条的要求（但数据处理者也可以使用其他形式的协议达到标准合同的效果，如 GDPR 标准合同条款）。

3) We suggest the CAC consider specifying exceptional circumstances to the requirement on the agreements between the data processors and the offshore recipients, e.g., where there is a need for financial institutions to provide data to offshore tax or banking authorities so as to comply with applicable foreign laws or international treaties/conventions, in which case, there is unlikely to be a contract being in place.

我们建议贵办公室考虑规定无需提供数据处理者和境外接收方之间合同的例外情形，例如，如果金融机构为遵守适用的外国法律或国际条约或公约，需要向境外税务或银行监管部门提供数据，这种情况下金融机构和境外监管部门之间不太可能会签订合同。

4) Article 9 (iii) restricts the re-transfer to a third-party. However, international financial institutions often transfer or subcontract certain data to its affiliates (e.g. for centralised functions) or its third party service providers to handle data processing activities. We would appreciate it if the CAC may confirm that "restriction" in Article 9(iii) does not intend to mean "prohibition". In this sense, provided that there is adequate visibility into that arrangement and controls in place with the third party, re-transfer should be permissible given that the financial institution has already satisfied itself and the CAC that the initial cross border transfer (taking into account the re-transfer which may/will take place) is appropriate, necessary and secure. We suggest the CAC consider amending the restriction on re-transfer to "restrictions on re-transfer, and/or data protection requirements and risk control measures in the circumstance of re-transfer by the data recipients (if applicable)".

《评估办法》第 9 条第（三）项限制境外接收方将出境数据再转移给其他第三方。然而，跨国金融机构通常会将部分数据传输或分包给其关联公司（例如，为在集团层面实施集中管理）或第三方服务提供商来进行数据处理活动。我们恳请贵办公室可以确认该条款中的"限制"并不意味着"禁止"。若这种理解是正确的，那么如果能够充分了解与该等第三方的安排和采取的控制措施，由于金融机构已经和贵办公室在首次跨境转移时已经确认跨境转移（同时可能的或将要发生的再转移也已纳入考虑）是适当、必要和安全的，再转移应当被允许。因此我们建议贵办公室考虑将"限制境外接收方将出境数据再转移给其他组织、个人的约束条款"修改为"境外接收方实施数据再转移情况下的转移限制和/或数据保护要求和风险控制措施（如适用）"。

5) Article 9(iv) mentions that security measures should be adopted where there is "substantial change in the actual controller or business scope of the overseas recipients" or "change in the legal environment of the country or region where the overseas recipient is located, which makes it difficult to guarantee data security" – this requirement is unclear as to what security measures the CAC is expecting from the data recipients to adopt on top of their then existing security measures. Given other security safeguards already imposed by this Article 9, and re-assessment will be triggered under Article 12 under such circumstances, we advocate the CAC to remove Article 9(iv). If the CAC decides to retain this requirement, we suggest the CAC clarify by whom and how the aforementioned two factors should be determined, and what additional security measures the overseas recipients are expected to adopt on top of their then existing security measures).

《评估办法》第 9 条第（四）项规定，如果"境外接收方在实际控制权或者经营范围发生实质性变化"，或者"所在国家、地区法律环境发生变化导致难以保障数据安全"，应当采取的安全措施。我们不清楚在该规定中，贵办公室期望数据接收方在其现有安全措施的基础上进一步采取什么安全措施。鉴于第 9 条已经施加了其他安全保障措施，第 12 条规定该等情况将触发数据出境评估的重新申报，我们建议贵办公室删除第 9 条第（四）项。如果贵办公室仍然决定保留这一要求，我们建议贵办公室进一步说明"境外接收方在实际控制权或者经营范围发生实质性变化"以及"所在国家、地区法律环境发生变化导致难以

保障数据安全”的判断标准和有权判断的机关，以及境外接收方在其现有安全措施的基础上，应当采取哪些额外的安全措施。

10. Standards and Procedure of Security Assessment
安全评估的标准和程序

As a transitional approach, we strongly advocate that firms' existing/ ongoing cross-border data flow before the effectiveness of the Measures be allowed to continue during the application process.
作为过渡性措施，我们强烈希望，在《评估办法》正式生效前，企业已经发生的或正在进行的数据跨境传输在申请安全评估的阶段能够得以继续。

1) Accepting and approving the application
受理和批准申请

Articles 7 and 11 provide that the CAC may determine whether to accept and approve the security assessment application. We encourage the CAC to make it clear that this is a permissive regime: provided that applicants are able to satisfy the criteria for risk identification, mitigation and control espoused in these Measures, we understand and expect that the default position will be to accept the application in relation to data transfers in most cases, and approve/permit accordingly.
《评估办法》第7条和第11条规定，贵办公室可决定是否受理和批准安全评估申请。我们希望贵办公室可以进一步明确，数据出境安全评估是一种对数据出境的许可性制度：如果申请人能够满足《评估办法》所规定的识别、降低和控制风险的标准，我们理解并期望贵办公室的基本态度是，在大多数情况下，贵办公室应当及时受理，并批准或允许数据的跨境转移。

2) Timetable for application approval
审查时限

Article 11 stipulates 45 business days (extendable to 60 business days) for reviewing the application. We strongly suggest the review timetable to be shortened significantly, e.g. by taking reference of the 15 business days as mentioned in the consultation draft of the Measures on Security Assessment of the Cross-Border Transfer of PI (Exposure Draft)（《个人信息出境安全评估办法（征求意见稿）》）issued in 2019.
《评估办法》第11条规定贵办公室将在受理后45个工作日内完成数据出境安全评估（特殊情况下可延长，一般不超过60个工作日）。我们希望尽可能地缩短审查时限，例如参考2019年发布的《个人信息出境安全评估办法（征求意见稿）》所规定的15个工作日。

3) Procedure of the application
申请流程

As with most other application process, we recommend the CAC to publish the detailed procedure or flow chart for the application and review for purpose of transparency.
与大多数其他申请流程类似，我们建议贵办公室可以公布申请和审查的详细程序或流程图，以提高透明度。

11. Effective Period for the Assessment Result
评估结果的有效期

Given the significant time involved in security assessment (including self-assessment to be conducted before regulatory assessment), we suggest the following changes be made to Article 12 relating to effective period for assessment result and re-assessment.
鉴于安全评估（包括监管评估前数据处理者的自评估）所需时间较长，我们建议对《评估办法》第 12 条有关评估结果有效期和重新评估的规定进行以下修改。

1) We would suggest the CAC remove the 2-year validity period for the security assessment and firms can provide appropriate notification and conduct re-assessment if there is a material change within the bounds of Article 12(i), 12(ii) and 12(iii). If the validity time is to be retained, we recommend extending the effective period for an assessment result from 2 years to say, 5 years, which is more reasonable considering that re-assessment will be conducted anyway during the effective period should the circumstances so request.
我们建议贵办公室删除安全评估结果的 2 年有效期，公司如果出现第 12 条第一款第（一）、（二）和（三）项范围内的重大变化，公司可以通知贵办公室并进行重新评估。如果保留有效期，我们建议延长有效期，例如延长到 5 年。我们认为在明确规定了有效期内的重新评估情形的前提下，适当延长有效期具有合理性。

2) We would suggest the CAC introduce a simplified procedure for renewal of the security assessment result (e.g., by confirm that the then existing outbound data transfer does not need to be suspended upon the expiry of the effective period of a security assessment result, provided that a re-assessment application has been made 60 business days before the expiry date).
我们建议贵办公室可以为重新评估制定一个简要程序（例如，在评估结果有效期届满前 60 日内已经进行过重新评估，那么在有效期届满时无需暂停数据跨境传输）。

3) We would suggest the CAC amend Article 12(i) so that only “material” change to the relevant matters concerned will trigger re-assessment.
我们请求贵办公室考虑将第 12 条第一款第（一）项规定的特定事项“发生变化”修改为“重大变化”，从而将触发重新评估的情形限制在有关事项的“重大变化”。

4) We would suggest the CAC clarify that re-assessment related application and review will only be on deviation from the previously reviewed matters, instead of a full review of the entire outbound data transfer plan, and accordingly shortening the review time for a re-assessment application.
我们希望贵办公室进一步解释，重新评估相关的申请和审查仅限于对先前审查事项发生偏离的范围内，而不是对整个数据跨境传输计划进行的全面审查，从而缩短重新评估申请的审查时间。

5) We would suggest the CAC allow data processors to continue data transfer during the re-assessment period or kicking off such re-assessment procedures way ahead of the proposed change so that the interruption to the business can be minimized.

我们建议贵办公室允许数据处理者在重新评估期间继续进行数据传输，或在第 12 条第一款规定的变更情形发生之前启动此类重新评估程序，尽可能降低对业务的负面影响。

6) We would suggest the CAC clarify what are the “other circumstances” provided under Article 12(3).
我们希望贵办公室可以明确说明第 12 条第一款第（三）项所规定的“其他情形”。

7) We would suggest the CAC changing the last two paragraphs of Article 12 to the following:
我们提议贵办公室将第 12 条第二款和第三款修改如下：

“If any of the above criteria applies and it is necessary to continue the original outbound data transfer activities (or if the effective period of the security assessment result expires), data processors shall re-apply for security assessment 60 working days before the proposed change (or before the expected expiration date, as applicable). The outbound data transfer may continue pending the outcome of the application.
Those who fail to re-apply for assessment in accordance with the provisions of this Article shall cease outbound data transfer activities.”
“如果上述第一款规定的情形发生，并且数据处理者需要继续开展原数据出境活动的（或者如果安全评估结果的有效期届满），则数据处理者应在第一款规定的变更发生前（或预期有效期届满前，如适用）60 个工作日重新申报安全评估。在申报审查期间，数据出境活动无需暂停。
未按本条规定重新申报评估的，应当停止数据出境活动。”

12. Revocation of approval
撤销审批

Article 16 provides that the CAC may “revoke the assessment result and notify the data processor” where, in the actual data handling process, outbound data transfer activities that have passed assessment no longer meet outbound data transfer security management requirements, we suggest the CAC include details and rationale for the revocation of the assessment result so that it gives clear guidance to the relevant data processor and other data processors for the outbound transfer process. We would also suggest incorporating grandfathering provisions to provide assurances that outbound data transfers that have previously been approved in accordance with these Measures would be exempted from any such revocation during the effective period of such approval, so as not to unfairly penalize entities whose failure to comply is attributable to changes to the requirements that become effective after the submission for approval was made.
《评估办法》第 16 条规定贵办公室在发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，有权撤销评估结果并通知数据处理者。我们建议贵办公室在通知中具体说明撤销评估结果的细节和原因，为数据处理者提供更为明确的指引。我们还希望可以在《评估办法》中确定“老人老政策”的方针，以确保已经根据《评估办法》获得批准的数据出境活动在有效期内不会因为数据出境安全管理要求的变更而被撤销，避免不公平地处罚那些提交申报后数据处境安全管理要求变更的情况。

Further, we recommend that a timeframe allowing adequate time for transition to a new solution be specified, or that at the very least acknowledges that a reasonable timeframe will be agreed, rather than expecting an instant halt to any data transfer activities. This would be disruptive to cross border business activities and could potentially be detrimental to the clients that financial institutions are servicing.

此外，我们建议规定允许数据处理者去满足新的数据处境安全管理要求的过渡期限，或者至少规定该等过渡期限将另行确定的原则性规定，而不是要求立即终止数据出境活动。否则这不利于企业的跨境业务活动，并可能对金融机构服务的客户造成潜在损害。

13. Grace Period
宽限期

International financial institutions usually need time to fully assess the legal and regulatory implications and take actions to comply with the relevant regulatory requirements. Most of our members would also need to go through internal authorisation and approval procedures for new data policies to take into effect. Therefore, we suggest the CAC consider providing a grace period before enforcing strict compliance with the relevant assessment procedures. We would suggest that a period of two years would be in line with grace periods provided for similar requirements globally, for example the EU's General Data Protection Regulation (the "GDPR").

跨国金融机构通常需要一定时间去全面评估法律和监管影响，并采取响应行动遵守相关监管要求。我们的大多数成员还需要通过内部授权和批准程序使得新的数据政策生效。因此，我们建议贵办公室在严格要求遵守有关数据出境评估程序前，考虑提供宽限期。我们希望建议采用国际通行的类似规定，例如 GDPR 规定了两年的宽限期。

In addition, for data transfers already occurring, it is not practical for data processors to re-do the assessment, so we suggest the CAC to clarify that the Measures will have no retroactive effect.

此外，对于已经出境的数据，数据处理者重新进行评估是不现实的，因此我们建议贵办公室明确《评估办法》没有溯及力。

ASIFMA greatly appreciates the CAC's consideration of the points and questions raised in this letter and would be pleased to discuss them in greater detail. If you have any questions, please contact Matthew Chan, Head of Public Policy and Sustainable Finance at mchan@asifma.org or +852 2531 6560. This submission was prepared by member PRC law firm Fangda Partners, ASIFMA, and its affiliates' members.

ASIFMA 非常感谢贵办公室考虑本函提出的观点和问题，并很乐意更详细地讨论这些问题。如果您有任何疑问，请联系公共政策和可持续财务部门总监 Matthew Chan（电邮：mchan@asifma.org，电话：+852 2531 6560）。本函由上海市方达律师事务所、ASIFMA 以及其会员共同撰写。

Faithfully,
顺颂时祺！

Matthew Chan
Head of Policy and Sustainable Finance, Asia Pacific
Asia Securities Industry & Financial Markets Association (ASIFMA)
亚洲证券业和金融市场协会