13 December 2021
2021 年 12 月 13 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

ASIFMA Headquarters
Unit 3603, Tower 2, Lippo Centre
89 Queensway
Admiralty, Hong Kong
Tel: +852 2531 6500

ASIFMA Singapore Office
One Raffles Quay, North Tower
Level 49, Unit 51B
Singapore, 048583
Tel: +66 6622 5970

Dear Sir/Madam:
尊敬的先生/女士：

RE: The Consultation Draft of the Network Data Security Management Regulations
关于：《网络数据安全管理条例（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 Network Data Security Management Regulations (《网络数据安全管理条例》) (the "**Regulations**")[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《网络数据安全管理条例（征求意见稿）》（"**本条例**"）提出意见和建议。

We respectfully set out here our queries and views on the draft Regulations for consideration by the CAC. In general, we have sought further clarifications on the draft which we believe may be open to different interpretations in the current form and have provided certain comments from a practical and industry perspective for your information and review. We have also provided our recommendations of certain articles of the Regulations. Unless otherwise specified, articles mentioned in this letter refer to the articles in the draft Regulations.
我们谨此列出我们对本条例草案的疑问及观点，供贵办公室考虑。总体而言，我们对我们认为现行草案中可能产生不同解释的内容寻求进一步澄清，并且从实践以及行业角度提供部分建议，供贵办公室考虑及审阅。我们同时也就本条例特定条款提供了我们的建议。除非另有说明，本函中提及的条款系指本条例草案中的条款。

---

[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/2021-11/14/c_1638501991577898.htm

Our comments and recommendations are structured as follows: (a) Section 1 contains the general and overarching comments to the Regulations; and (b) Section 2 contains the key comments to the Regulations and specific suggestion on certain articles.
我们的意见及建议将分成两部分：（1）第 1 节包括对本条例的一般及整体意见；以及（2）第 2 节包括对本条例的关键意见以及对于特定条款的具体建议。

1. General and Overarching Comments
一般及整体意见

1.1 To Align with the PIPL, the DSL and the CSL
与《个人信息保护法》、《数据安全法》以及《网络安全法》保持一致

The Regulations are implementing regulations issued under the umbrella of the Cybersecurity Law ("**CSL**"), the Data Security Law ("**DSL**") and the Personal Information Protection Law ("**PIPL**", together with the CSL and DSL, the "**Laws**"). However, we note that the Regulations broaden and make more onerous the requirements under the Laws in certain significant respects. The examples include without limitation:

本条例系基于《网络安全法》、《数据安全法》以及《个人信息保护法》（与《网络安全法》及《数据安全法》合称为"**数据法律**"）所制定的实施条例。但是，我们注意到本条例在特定重要方面扩大了数据法律的要求且使其更加复杂，包括但不限于：

(a) Article 2 of the Regulations expands the scope of extra-territorial application; and
本条例第 2 条扩大了域外适用效力；以及
(b) Article 33 of the Regulations requires regulatory approval for sharing or trading of important data or outsourcing the processing of important data, which is a brand new approval that does not have sufficient legal support under the three Laws.
本条例第 33 条要求共享或交易重要数据或委托处理重要数据的，需要获得监管同意，这是一项全新的同意要求，且在三部数据法律中没有足够的法律支持。

We believe the data security requirements under the Regulations should studiously follow the scope and data security framework laid down in these three Laws and should not expand the scope of or deviate from the general framework. We would respectfully suggest that the requirements under the Regulations should be consistent with those set out in the relevant Laws.
我们相信，本条例项下的数据安全要求应当严格遵循通过三部数据法律所确立的范围以及数据安全框架，且不应当扩展其适用范围或偏离基本框架。我们谨此建议本条例项下的要求应当与相关数据法律项下的要求保持一致。

1.2 To Avoid the Ambiguity in the Regulations
避免本条例中的歧义

We note that certain terminologies used in the Regulations do not align with that used under the Laws and other existing measures and standards. Overlapping and indistinct terms, and inconsistent use of undefined terms might cause ambiguity. We respectfully suggest that the CAC should clarify such definitions and their relationships, the examples of which include:
我们注意到，本条例中使用的特定术语未与数据法律、其他现有规定及标准中使用的术语保持一致。重叠或不清晰的概念，以及对未定义词汇不一致的使用将可能导致歧义。我们谨此建议贵办公室应当澄清该等定义及其关系，例如：

(1) what is the relationship between "personal information ("**PI**")" and "data" or "important data" (please also refer to Section 2.2);
"个人信息"与"数据"或"重要数据"关系（亦请参考第 2.2 节）；

(2) the terms "general data", "important data" or "core data" used in Article 5 and the relationship/differences among these terminologies; and
本条例第 5 条所使用的"一般数据"、"重要数据"或"核心数据"的定义及其关系/不同；以及

(3) the scenarios triggering CAC-led security assessment is not consistent with the consultation draft of the Measures for the Security Assessment of Data Outbound Transfer (the "**Data Outbound Transfer Consultation Paper**") and are more aligned with the DSL, CSL and the PIPL. We seek confirmation that the scenarios triggering CAC-led security assessment are no more than what are prescribed in the draft Regulations. However, it is still not clear how the 1 million individual threshold would be determined, which is mentioned several times in the Regulations. We recommend that the amount is based on a specified period of time (e.g. 6 months or 1 year). We would also like to recommend CAC consider our separate response paper in relation to the Data Outbound Transfer Consultation Paper submitted to CAC in this regard.
本条例项下触发贵办公室组织的安全评估的情形与《数据出境安全评估办法（征求意见稿）》（"**《数据出境征求意见稿》**"）中规定的情形不一致，但更符合《数据安全法》、《网络安全法》以及《个人信息保护法》。我们特此向贵办公室确认，触发该等安全评估的情形将不会多于本条例草案中所列明的情形。此外，一百万个人的数量门槛将如何被认定亦尚不明确，该等门槛在本条例中被反复提及。我们建议该门槛应当是基于特定时间段（例如 6 个月或 1 年）。我们也建议贵办公室考虑我们就《数据出境征求意见稿》所另行向贵办公室呈递的意见函件。

1.3 To Align and Coordinate with the Sectoral Regulators
与行业主管机构保持一致并协调

Take the financial industry as an example. The Regulations should take into consideration of financial institutions' existing obligations under various applicable laws (e.g. anti-money laundering and incident reporting) and align with sectoral rules. We recommend a streamlined regulatory framework where financial regulators are responsible for the sector-wide data security rules and interacting with financial institutions. Financial regulators should further coordinate with the CAC on data security matters.

以金融行业为例。本条例应当考虑金融机构在不同适用法律项下现有的义务（例如反洗钱及事件报告），并且与该等行业规则协调。我们建议采用更简洁的监管框架，在该等框架之下，金融监管部门将负责行业内的数据安全规定以及与金融机构沟通。金融监管机构应当进一步与贵办公室就数据安全事务进行协调。

2. Key Comments to the Regulations and Specific Suggestions on Certain Articles
对本条例的关键意见以及对特定条款的具体建议

We respectfully set out our specific suggestions in the appendix, and in particular, we would like to highlight some key comments that are of great concern from our members.

我们在附件中谨此列出我们的具体建议，我们同时希望特别强调我们会员特别关注的关键意见。

2.1 Scope of Application – Extra-territorial Effect (Article 2)
适用范围 – 域外效力（第 2 条）

The Regulations broaden the application of the Laws beyond the Laws' original scope, as well as introduce new terminologies not found in the Laws themselves. For example, Article 2 of the Regulations:

本条例在数据法律原有适用范围基础上，扩大了对数据法律的适用，同时也引入了在数据法律中未出现的新术语。例如，本条例第 2 条：

(a) specifies that the scope of the Regulations to be processing of "personal and organizational data" within and outside of the PRC. However, currently (aside from national security impacting processing) the Laws only apply extra-territorially in relation to processing of PI which relates to individuals within the PRC and it's not clear how the Regulations would operate alongside the Laws if the Regulations do not have the effect of expanding the effect of the DSL and CSL to apply to data processors located outside of the PRC; and

明确本条例的适用范围为在中国境内外处理"个人和组织数据"。但是，目前除了影响国家安全的处理活动，数据法律仅在处理中国境内自然人的个人信息时，会触发域外效力。如果本条例不具有扩大《数据安全法》和《网络安全法》效力并使其适用于位于中国境外的数据处理者的效力，本条例如何与数据法律一起被落实的方式尚不清楚；以及

(b) introduces four general extra-territoriality triggers – these four triggers expand beyond the reach of the existing PIPL extra-territoriality triggers and they both now apply not only in relation to individuals but also to 'organizations' and introduce a wholly new trigger for extra-territorial reach not found in the original Laws – namely, the processing of important data that relates to the PRC outside of the PRC.
介绍了触发域外效力的四种情形 – 该等四种情形超出了现有《个人信息保护法》的域外效力触发情形，并且现在他们不仅适用于个人，也同时适用于"组织"，此外引入了较原数据法律而言全新的触发情形 – 也就是，在中国境外处理涉及境内的重要数据。

If Article 2 is adopted in its current state, these Regulations would be inconsistent with and broader than the original Laws that they seek to implement/clarify. In addition, Article 2 would potentially cause the Regulations (and by extension, the Laws) to apply extraterritorially irrespective of whether the processing entity has onshore establishments and/or operations or not.
如果第 2 条以现有形式正式发布，本条例拟实施或澄清之内容将会与原数据法律不符且较之更广。此外，第 2 条将可能导致本条例（随之而来的，数据法律）在域外适用而无论处理主体是否在境内有实体或运营。

One further effect of this would be a need to ensure that offshore businesses and operations serving the PRC not only comply with the laws of their respective jurisdictions but also comply with the PRC data laws as if they were entities set up within the territory of the PRC. This will very likely lead to a conflict of obligations and a higher regulatory bar to be crossed prior to providing products or services into the PRC. Ultimately, this is likely to generally discourage global businesses from offering products and services into the PRC to the detriment of Chinese businesses and consumers.
一个深层次的影响可能是，服务中国但是位于境外的业务或运营主体需要确保不仅符合他们各自司法辖区的法律，同时也需要符合中国的数据相关法律，如同他们是在中国境内设立的实体。这将非常可能导致义务的冲突和在向中国提供产品或服务之前，更高的监管壁垒。最终，这将可能很大程度上阻碍国际业务实体向中国提供产品或服务，而这将最终有损于中国商业活动以及消费者。

We therefore respectively suggest that the CAC should align the scope of the Regulations to be consistent with the original scope of the Laws and the CAC should also consider the extra-territorial

application of other similar legislation globally, for example the General Data Protection Regulation (the "**GDPR**"). Please refer to Appendix for our detailed recommendation on how Article 2 can be amended for consistency with the Laws.
因此，我们谨此建议贵办公室应当将本条例的适用范围与数据法律的原适用范围保持一致，贵办公室也应考虑其他类似国际立法项下的域外适用规定，例如《通用数据保护条例》（"**GDPR**"）。就我们对第 2 条应当如何调整以保证与数据法律一致的具体建议，请参考附件。

2.2 Regulation of Protection of PI vs Important Data vs Critical Information Infrastructure ("CII") (Article 9 and Article 26)
关于个人信息 vs 重要数据 vs 关键信息基础设施（"CII"）的规定（第 9 条及第 26 条）

The Regulations do not seem to draw clear lines between different concepts, which include:
本条例并未在不同概念之间进行明确区分，包括：

(a) according to Article 9 of the Regulations, the system processing important data shall meet the requirements of both Multi-level Protection Scheme ("**MLPS**") Level 3 and CII; and
根据本条例第 9 条，处理重要信息的系统应当同时满足三级以上网络安全等级保护（"**等保要求**"）和 CII 安全保护要求；以及

(b) according to Article 26 of the Regulations, data processors that process PI of more than one million individuals will be subject to regulation under Chapter 4 (Security of Important Data) of the Regulations, which applies to "Important Data".
根据本条例第 26 条，处理一百万人以上个人信息的数据处理者将需遵循适用于重要数据的本条例第四章（重要数据安全）的规定。

We believe that such requirements may potentially be significantly onerous and burdensome on the regulator and the data processors, given the expected number of participants that would satisfy such requirements and therefore be subject to the Regulations. In particular, our members are of the view that:
我们相信，考虑到可能符合该等要求而被要求适用本条例相关规定的参与主体的数量可能非常庞大，该等要求可能对监管机构及数据处理者而言极度复杂及任务繁重。尤其是，我们的会员认为：

(a) the criteria and process for MLPS classification and CII designation and protection are established in separate rules respectively and it lacks legal basis to require systems processing important data to meet both MLPS level 3 and CII requirements; and
等保要求分级的标准和流程，以及 CII 的认定和保护系通过不同的规定分别建立。如果要求处理重要信息的系统应当同时满足三级以上等保要求和 CII 安全保护要求，缺乏法律基础；以及

(b) the requirements under Chapter 4 of the Regulations which are designed to ensure the security of important data may not be as relevant in the context of the processing of large amounts of PI (which is represented by the 1 million individual requirement). Internationally, PI protection is for reasons such as privacy and personal interests protection and has no connection with national security. Grouping PI with national security data is not compatible with global norms or the spirit in multi-lateral agreements such as CPTPP, RCEP and DEPA. Our members note that data processors are already required to carry out data security assessment every year while the PI processors are already under the requirements of performing a PI protection impact assessment according to Articles 55 of the PIPL.
本条例第四章项下的要求系出于确保重要信息的安全的目的所设计，该等出发点可能与处理大量个人信息（系指超过一百万人的要求）的情形不相关。在国际上，个人信息保护系出于隐私保护、个人利益保护等原因，但与国家安全并无关系。将个人信息与国家安全数据打包的做法与国际惯例存在出入，也与多边协议（例如 CPTPP、RCEP 以及 DEPA）的精神违背。我们的成员注意到，数据处理者已经被要求每年开展数据安全评估，而个人信息处理者也已被《个人信息保护法》第 55 条要求开展个人信息保护影响评估。

Besides, it remains unclear to us with respect to the relationship between PI and important data. We note that the consultation draft of Information Security Technology - Guidelines for Identifying Important Data ("**Important Data Guidelines**") issued by the Standardization Administration of China in September this year explicitly points out that important data does not include PI, while statistical or derivative data that is generated based on massive PI may fall within the scope of important data. We suggest the CAC clarify in the Regulations that whether there will be overlaps between PI and important data and if the answer is yes, provide more guidance to data processors on how to properly discharge their obligations.
此外，我们尚不清楚个人信息与重要数据之间的关系。我们注意到，全国信息安全标准化技术委员会于今年 9 月发布的《信息安全技术 重要数据识别指南（征求意见稿）（"**《重要数据指南》**"）明确指出，重要数据不包括个人数据，但是基于海量个人信息产生的统计数据、衍生数据可能落入重要数据的范畴。我们建议贵办公室澄清，在本条例中是否可

能存在个人信息与重要数据重叠的情况；如是，就数据处理者如何合理履行其义务提供更多指导。

2.3 Definition and Ground for Separate Consent (Article 21 and Article 73(8)) 单独同意的定义及依据（第 21 条及第 73 条第（八）项）

The definition of separate consent set out in Article 73(8) of the Regulations provides that consent needs to be obtained for "each PI" processed by the data processor. This could potentially mean that each separate piece of information obtained from an individual (e.g. name, address, contact number) would require a separate consent, which we do not believe to be the intention. If a separate consent were to be required for each PI, this would potentially be extremely administratively burdensome. We would therefore suggest that clarificatory amendments be made to the definition to provide that a single separate consent for the processing of such information would be sufficient.
本条例第 73 条第（八）列明了单独同意的定义，指出数据处理者应就处理的"每项个人信息"取得同意。这将意味着，从自然人处获得的每个单独的个人信息（例如姓名、地址、联系方式）都会被要求获得单独同意，但我们理解这应该不是监管的意图。如果每项个人信息都需要获得单独同意，这可能导致在管理上极其繁琐。因此，我们建议对定义进行澄清性质的调整，以明确为处理该等信息，一次性单独同意即可满足要求。

Besides, Article 21 of the Regulations provides, among other things, that separate consents shall be obtained from individuals for processing of sensitive personal information. We would appreciate if CAC could confirm that the separate consent requirement for processing of PI is only required if the lawful processing of such PI would be based on consent. In circumstances where the data processor would be relying on other grounds for such processing (e.g. those under Article 13 of the PIPL, e.g. for entering into or performance of an agreement), it would not be necessary to obtain such separate consent. We believe this is the view represented by Article 21 of the Regulations if reading in conjunction with Articles 13 and 14 of the PIPL, but would appreciate CAC's confirmation on this.
此外，本条例第 21 条明确，除其他事项之外，在处理自然人的敏感个人信息时应获得单独同意。我们希望贵办公室可以确认，个人信息处理的单独同意要求仅在同意构成处理该等个人信息的合法前提时适用。如果数据处理者系依赖于其他原因处理个人信息（例如根据《个人信息保护法》第 13 条所列明的其他原因，例如订立或履行合同），并不需要获得该等单独同意。如果同时参考《个人信息保护法》第 13 条及第 14 条，我们认为这一观点也在本条例第 21 条得到印证，但我们希望贵办公室可以就这一点进行确认。

2.4 Identification of Important Data and Related Regulation (Article 73(3))
重要数据识别及其监管（第 73 条第（三）项）

We note that Article 73(3) provides a non-exclusive list on what would constitute "important data" for the purposes of the Regulations, which is helpful in providing additional colour. We hope that greater clarity could be provided to organizations across different industries and the public regarding the timing, scope and attributes of sectoral regulators' forthcoming important data catalogues, as the inclusion of certain types of data in these documents will have significant implications for businesses and their partners. Additionally, we believe the definition for "important data" should reference the draft CAC Data Security Management Measures in 2019 to exclude enterprise production management and internal business operations data.

我们注意到第 73 条第（三）项列明了，为本条例之目的，可能被认定为"重要数据"的非穷尽式清单，该等清单在提供更多信息方面确实非常有帮助。我们希望，贵办公室可以向不同行业及社会上组织就行业主管机构即将颁布的重要数据目录的时点、范围以及特征提供更多澄清，因为在该等目录中加入特定数据类型将会对业务以及合作方产生重大影响。此外，我们相信"重要数据"的定义将会参考贵办公室在 2019 年颁布的《数据安全管理办法（征求意见稿）》，即将企业生产经营和内部管理信息排除在重要数据之外。

2.5 Outbound Data Transfer (Article 35 and Article 39)
数据出境（第 35 条及第 39 条）

The Regulations expand the PIPL cross-border requirements to all forms of data, which lacks sufficient legal basis under the Laws. Besides, the Regulations also set out the obligations of data processors when providing data outside the territory of the PRC, including, to sign a contract to supervise the use of data by data recipients, to bear liability if the outbound data transfer causes damage to the legitimate rights and interests of individuals or organizations or the public interest, which are not equitable and fair from our members' perspective.

本条例扩大了《个人信息保护法》项下关于跨境的要求，而使得该等要求适用于所有类型的数据，该等扩展缺乏数据法律项下足够的法律依据。此外，本条例也列明了数据处理者在向中国境外提供数据时应当履行的义务，包括签署合同以对数据接收方的数据使用行为进行监督，在数据出境导致个人或组织的合法权益或公共利益受到损害时承担相应的责任。我们的成员认为，该等义务存在不合理、不公平的问题。

We would also like to recommend CAC consider our separate response paper in relation to the Data Outbound Transfer Consultation Paper submitted to CAC on 28 November 2021. Separately, we would appreciate it if the CAC could confirm that the scenarios triggering CAC-led security

assessment for cross-border transfer of data are not beyond the ones described in Article 37 of the draft Regulations and align the approaches and requirements for CAC-led security assessment between the Regulations and the Data Outbound Transfer Consultation. For our detailed recommendations to the Regulations, please refer to the Appendix.
我们也建议贵办公室考虑我们于 2021 年 11 月 28 日就《数据出境征求意见稿》所另行准备的意见函件。此外，我们希望贵办公室可以确认，触发贵办公室组织实施的安全评估的数据出境情形将不会超过本条例草案第 37 条所载明的情形。此外，就贵办公室组织实施的安全评估的方式及要求，贵办公室将会在本条例以及《数据出境征求意见稿》之间保持一致。就我们对本条例具体的建议，请见附件。

2.6 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 requirements. We would suggest that a period of two years would be in line with the grace periods provided for similar requirements globally, for example the GDPR.

跨国金融机构通常需要一定时间对法律和监管影响进行全面评估，并采取响应行动以遵守相关监管要求。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要求严格遵守有关规定之前，考虑提供宽限期。我们将建议采用两年的期限，这与国际通行的类似规定保持一致，例如 GDPR。

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 members.

ASIFMA 非常感谢贵办公室考虑本函提出的观点和问题，并很乐意对此进行更详细的讨论。如果您有任何问题，请联系公共政策和可持续财务部门总监 Matthew Chan（电子邮箱：mchan@asifma.org；电话：+852 2531 6560）。本函由上海市方达律师事务所、ASIFMA 以及其成员共同撰写。

Faithfully,
顺颂时祺！

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

Appendix – Specific Suggestions on Certain Articles
附件 – 特定条款的具体建议

Article 条款	Comments 意见	Recommendation 建议
Article 2 These Regulations apply to the use of networks to conduct data processing activities and the supervision and management of network data security within the territory of the People's Republic of China. **第二条** 在中华人民共和国境内利用网络开展数据处理活动，以及网络数据安全的监督管理，适用本条例。 These Regulations shall apply to the processing of the data of individuals and organizations in the People's Republic of China undertaken overseas under any of the following circumstances: 在中华人民共和国境外处理中华人民共和国境内个人和组织数据的活动，有下列情形之一的，适用本条例：	As mentioned in Section 2.1, Article 2 expands the scope of extra-territorial application beyond the scope of the original Laws in the following manner: 如正文第 2.1 节所述，第 2 条在数据法律的基础上扩大了域外适用效力，如： (1) the scope to be processing of "personal and organizational data" within and outside of the PRC, which lacks legal basis; and 该条规定适用范围为在中国境内外处理"个人和组织数据"，缺少法律依据； (2) four general triggers introduced in the Regulations, one of which also covers the processing of important data.	We recommend that the Article 2 follow the scope laid down in the PIPL, scale back to covering only PI and remove bullet (3). We suggest changing Article 2 to the following to be consistent with the PIPL: 我们建议第 2 条遵循《个人信息保护法》规定的适用范围，将适用情形缩小到个人信息，并且删去第二款第（三）项。为此，我们建议对第 2 条作出如下修改，使其与《个人信息保护法》的规定一致： "**Article 2** These Regulations apply to the use of networks to conduct data processing activities and the supervision and management of network data security within the territory of the People's Republic of China.

Article 条款	Comments 意见	Recommendation 建议
(1) for the purpose of providing products or services within the territory; （一）以向境内提供产品或者服务为目的； (2) analyze and evaluate the behaviors of individuals or organizations within the territory; （二）分析、评估境内个人、组织的行为； (3) involving the processing of important data within the territory; or （三）涉及境内重要数据处理； (4) other circumstances stipulated by laws or administrative regulations. （四）法律、行政法规规定的其他情形。 These Regulations do not apply to the data processing activities that natural persons conduct for their personal or family affairs.	该条规定的触发域外适用效力的四种情形包括“涉及境内重要数据的处理”。 Such expansion may catch numerous offshore entities to comply with the Regulations, which is not reasonable and feasible. 这种扩大可能会导致大量境外机构需要遵守本条例，这可能是不合理也不实际的。 Besides, we suggest CAC take into consideration of the fact that intra-group collaboration (including without limitation the human resources management) is very common and important for international financial institutions. If the intra-group transfers in the course of ordinary business is caught by the Regulations, the implications might be tremendous, making it too burdensome and less efficient for the operation. Therefore, we suggest CAC	**第二条** 在中华人民共和国境内利用网络开展数据处理活动，以及网络数据安全的监督管理，适用本条例。 These regulations ~~shall~~ also apply to the processing of the personal information of natural persons ~~data of individuals and organizations~~ within the People's Republic of China that is undertaken outside the People's Republic of China if such activities are: 在中华人民共和国境外处理中华人民共和国境内自然人的个人信息~~和组织数据~~的活动，有下列情形之一的，适用本条例： (1) for the purpose of providing products or services to natural persons within the territory; （一）以向境内自然人提供产品或者服务为目的；

Article 条款	Comments 意见	Recommendation 建议
自然人因个人或者家庭事务开展数据处理活动，不适用本条例。	provide exceptions for such scenario in Article 2. 此外，我们建议贵办公室考虑，集团协同（包括但不限于人力资源管理）对于国际金融机构而言是非常普遍且重要的。若本条例适用于正常商业经营过程中的集团内数据传输，其影响将是巨大的，会对企业经营带来过重的负担并降低效率。因此，我们建议贵办公室可以在第2条中豁免对此类情形的适用。	(2) conducted to analyze and evaluate the behaviors of natural persons ~~individuals or organizations~~ within the territory; or （二）分析、评估境内自然人~~个人、组织~~的行为；或 ~~(3) involving the processing of important data within the territory; or~~ ~~（三）涉及境内重要数据处理；~~ (4~~3~~) in any of the other circumstances stipulated by laws and administrative regulations. … （~~四~~三）法律、行政法规规定的其他情形。…” We also suggest CAC provide exception for intra-group transfer in ordinary course of business of international financial institutions. 此外，我们希望贵办公室可以对跨国金融机构正常业务经营中发生的集团内数据传输行为提供豁免。

Article 条款	Comments 意见	Recommendation 建议
Article 5 The State is to establish a classified and graded data protection system. According to data's impact on and importance to national security, public interests or the legal rights or interests of individuals or organizations, data is classified into general data, important data and core data, and different protection measures are taken for different levels of data. **第五条** 国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。 The State implements focused protection for personal information and important data, and strict protection for core data. 国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。 All regions and departments shall implement classified management of data in their own	The Regulations serve as implementation measures for the Laws, and should studiously follow the scope and data security framework laid down in the three laws and not expand scope and deviate from the general framework. 本条例作为数据法律的实施条例，应当严格遵循数据法律规定的范围和数据安全保护框架，不应扩大适用范围或偏离该等框架。 We support the promotion of sound data governance practices where data classification is an integral component, and government and companies all have the flexibility in classifying their own data appropriate to their respective needs and sectors. Given that they serve different purposes, we would recommend that government data and commercial data also be classified separately. For commercial data classification, companies should be permitted take the lead in determining the	We recommend removing the type of "general data" since it is not specified in the Laws. If it is not acceptable, we recommend clarifying that general data are the network data other than important data or core data. Besides, the Regulations and other implementation rules to be issued in the future (if any) shall not introduce additional obligations surrounding such general data except for those minimum requirements in relation to data protection. 我们建议删除"一般数据"这一未被数据法律提及的类别，如果上述建议不可行，我们建议贵办公室可以明确一般数据是重要数据和核心数据以外的网络数据。同时，除了数据保护相关的最低要求外，本条例以及将来发布和其他实施规则（如有）不应针对一般数据对数据处理者施加额外义务。 Besides, we recommend that a list/catalogue shall be prepared and attached to the Regulations or published separately so as to identify the type of the data and we sincerely

Article 条款	Comments 意见	Recommendation 建议
regions and departments as well as the relevant industries and fields in accordance with the State's data classification and grading requirements. 各地区、各部门应当按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理。	appropriate classification levels for data under their control. 我们对监管建立健全数据治理架构表示支持，其中数据分类分级制度是不可或缺的组成部分，政府和企业都可以灵活地根据各自的需求和所在行业对自己的数据进行分类。鉴于政府数据和企业商业数据的用途不同，我们建议将政府数据和商业数据分别进行分类。对于商业数据的分类，应允许企业在确定其所控制的数据的合适类别等级时发挥主导作用。	expect a clear boundary will be provided for the different types of data and if there will be overlaps under certain circumstances, we suggest the CAC specifying such circumstances and overlaps. We also suggest industry regulators and regional government work in consultation with industry when carrying out data classification work. 此外，我们建议编制一份明确不同数据类型的清单或目录，作为本条例的附件或单独发布。我们真诚希望不同类型的数据之间具有明确的界限，如果不同类别的数据可能会互相转换或者重叠，我们建议贵办公室能够明确此类情况和重叠的数据种类。同时，我们也建议行业监管机构和地方政府在执行数据分类工作时与相关行业单位进行沟通讨论。 We suggest changing Article 5 to the following: 我们建议将第 5 条修改如下：

Article 条款	Comments 意见	Recommendation 建议
		"**Article 5** The State is to establish a classified and graded data protection system for government owned data. According to data's impact on and importance to national security, public interests or the legal rights or interests of individuals or organizations, ~~data is classified into~~ the State will issue the catalogue of important data and core data and the data other than those listed in the published catalogue shall be classified as general data. ~~and~~ Different protection measures are taken for different levels of data. **第五条** 国家对政府数据建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，国家对重要数据、核心数据发布数据清单，未列入数据清单的~~将~~数据~~分~~为一般数据~~、重要数据、核心数据~~，不同级别的数据采取不同的保护措施。

Article 条款	Comments 意见	Recommendation 建议
		The State implements focused protection for personal information and important data, and strict protection for core data. 国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。 All regions and departments shall implement classified management of data in their own regions and departments as well as the relevant industries and fields in accordance with the State's data classification and grading requirements. 各地区、各部门应当按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理。"
Article 6 Data processors shall be responsible for the security of the data processed by them, perform data security protection obligations, accept supervision by the government and the public, and take on social responsibilities.	We strongly recommend that mandatory requirements should be clearly laid out in laws and regulations. Recommended national standards should not be forced onto companies through direct reference by laws and regulations. It's important to make sure companies have flexibility to choose approaches best suited to them and	We suggest changing Article 6 to the following: 我们建议将第 6 条修改如下： "**Article 6** Data processors shall be responsible for the security of the data processed by them, perform data security protection obligations, accept supervision by

Article 条款	Comments 意见	Recommendation 建议
第六条 数据处理者对所处理数据的安全负责，履行数据安全保护义务，接受政府和社会监督，承担社会责任。 Data processors shall establish and improve their data security management systems and technical protection mechanisms in accordance with the provisions of the relevant laws, administrative regulations and mandatory requirements of national standards. 数据处理者应当按照有关法律、行政法规的规定和国家标准的强制性要求，建立完善数据安全管理制度和技术保护机制。	recommended standards should be treated as one of industry best practice for companies to reference or partially adopt. 我们强烈建议在法律法规中明确指出强制性要求。推荐性国家标准不应被法律法规直接引用从而强制适用于企业。我们认为，确保企业能够灵活采取最适合自己的方式是非常重要的，推荐性国家标准应作为行业的最佳实践之一，供企业参考或部分采用。 Furthermore, considering China's active participation in global standard setting efforts, we strongly recommend that China recognize and adopt international standards as much as possible and align approaches with international standards that are developed in an open, inclusive and transparent manner with multiple stakeholders' inputs. 此外，考虑到中国在全球标准制定工作中的积极参与，我们强烈建议中国尽可能多地承认和采用国际标准，与	the government and the public, and take on social responsibilities. **第六条** 数据处理者对所处理数据的安全负责，履行数据安全保护义务，接受政府和社会监督，承担社会责任。 Data processors shall establish and improve their data security management systems and technical protection mechanisms in accordance with the provisions of the relevant laws, administrative regulations and requirements in national mandatory standards ~~mandatory requirements of national standards~~. 数据处理者应当按照有关法律、行政法规的规定和强制适用的国家标准的~~强制性~~要求，建立完善数据安全管理制度和技术保护机制。"

Article 条款	Comments 意见	Recommendation 建议
	那些以开放、包容和透明的方式制定的，且有多个利益相关者参与的国际标准保持一致。	
Article 8 Any individual or organization conducting data processing activities shall comply with laws and administrative regulations, respect social morals and ethics, and shall not: **第八条** 任何个人和组织开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动： (1) endanger national security, honor or interests, or disclose state secrets or work secrets; （一）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密； (2) infringe upon the reputation, privacy, copyright or other legitimate rights or interests of others;	Those behaviors are either civil or criminal offences that are sufficiently covered in existing laws and regulations. 第 8 条所列行为属于现行法律法规已经充分规定的民事违法或刑事犯罪行为。 We would like to highlight that financial institutions already perform anti-money laundering (AML) and counter-terrorism finance (CTF) obligations before providing services to clients, and those should be viewed as sufficient due diligence efforts. Any further due diligence required on clients should come through financial regulators' AML and CTF requirements. 我们仍想强调，金融机构已经被要求在向客户提供服务之前履行反洗钱（AML）和打击资助恐怖主义（CTF）的义务，这些应被视为充分的	We suggest deleting the Article as those behaviors are either civil or criminal offences that are sufficiently covered in existing laws and regulations. 我们首先建议删除该条，因为这些行为属于现行法律法规已经充分规定的民事违法或刑事犯罪行为。 If it is not deleted, we suggest the CAC (1) confirm that financial institutions are not expected to perform additional due diligence on clients or beneficiaries in financial transactions beyond AML and CTF requirements imposed by financial regulators, and (2) remove the wording of "or should have known" in the second paragraph which will impose a stringent and additional due diligence requirement on the financial institutions once the Regulations enter into effect.

Article 条款	Comments 意见	Recommendation 建议
（二）侵害他人名誉权、隐私权、著作权和其他合法权益等； (3) obtain data by theft or other illegal means; （三）通过窃取或者以其他非法方式获取数据； (4) illegally sell or provide data to others; （四）非法出售或者非法向他人提供数据； (5) make, release, copy or disseminate illegal information; or （五）制作、发布、复制、传播违法信息； (6) conduct any of the other activities prohibited by laws or administrative regulations. （六）法律、行政法规禁止的其他行为。	尽职调查工作。因此，我们认为，金融机构对客户的任何进一步尽职调查都应按照金融监管机构所要求的反洗钱和打击资助恐怖主义的义务进行。	若贵办公室仍然认为需要保留，我们建议贵办公室(1) 确认金融机构不需要在金融交易中对客户或受益人履行除金融监管机构规定的反洗钱和打击资助恐怖主义要求以外的尽职调查，以及(2) 删除第二款规定的"或者应当知道"，否则一旦本条例生效，这将对金融机构施加更严格的额外尽职调查要求。

Article 条款	Comments 意见	Recommendation 建议
No individual or organization that knows or should have known that another individual or organization is engaged in any of the activities set forth in the preceding paragraph shall provide this individual or organization with any technical support, tools, programs, marketing or advertising, payment clearing or any other services. 任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。		
Article 9 Data processors shall take necessary measures such as backup, encryption and access control to protect data from being leaked, stolen, tampered with, damaged, lost or illegally used, respond to data security incidents, prevent illegal and criminal activities that target or use data, and maintain the integrity, confidentiality and availability of data. **第九条** 数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢	As mentioned in Section 2.2, Multi-level Protection Scheme (MLPS) Regulations (draft) (《网络安全等级保护条例（征求意见稿）》) and CII Protection Regulations (《关键信息基础设施安全保护条例》) establish the criteria and process for MLPS classification and CII designation respectively, and should be followed as the authoritative guidance when it comes to MLPS classification and CII designation. Sweepingly requiring systems processing important data to meet MLPS	We suggest Article 9 should be removed and in case that this article will be retained, change Article 9 to the following: 我们建议删除第 9 条。若第 9 条仍然被保留，我们建议对该条修改如下： "**Article 9** Data processors shall take necessary measures such as backup, encryption and access control to protect data from being leaked, stolen, tampered with, damaged, lost or illegally used, respond to data security incidents, prevent illegal and

Article 条款	Comments 意见	Recommendation 建议
失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。 Data processors shall strengthen security protection for their data processing systems, data transmission networks, and data storage environments in accordance with the requirements of classified protection of cyber security. Systems processing important data shall, in principle, meet the Level 3 or higher requirements of classified protection of cyber security and the requirements of security protection for critical information infrastructures. Systems processing core data shall be strictly protected in accordance with relevant regulations. 数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设	level 3 and CII requirements lacks legal basis. 如正文第 2.2 节所述，《网络安全等级保护条例（征求意见稿）》和《关键信息基础设施安全保护条例》为网络安全等级的分类和 CII 的判定明确了标准和流程，并应作为网络安全等级分类和 CII 判定的权威指引。因此，全面要求处理重要数据的系统满足三级以上网络安全等级保护和 CII 安全保护的要求，欠缺法律依据。	criminal activities that target or use data, and maintain the integrity, confidentiality and availability of data. **第九条** 数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。 Data processors shall strengthen security protection for their data processing systems, data transmission networks, and data storage environments in accordance with the requirements of classified protection of cyber security. ~~Systems processing important data shall, in principle, meet the Level 3 or higher requirements of classified protection of cyber security and the requirements of security protection for critical information infrastructures. Systems processing core data shall be strictly protected in accordance with relevant regulations.~~

Article 条款	Comments 意见	Recommendation 建议
施安全保护要求，处理核心数据的系统依照有关规定从严保护。 Data processors shall use encryption to protect important data and core data. 数据处理者应当使用密码对重要数据和核心数据进行保护。		数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护~~，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护~~。 Data processors shall use encryption to protect important data and core data. 数据处理者应当使用密码对重要数据和核心数据进行保护。”
Article 10 When a data processor discovers that any network product or service it uses or provides has any security vulnerability or loophole, or poses any risk such as threatening national security or endangering public interests, such data processor shall immediately take remedial measures. **第十条** 数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公	It is recommended that the Regulations take a risk and principles-based approach and allows companies the flexibility to take most suitable and appropriate measures to address such findings. 我们建议本条例以风险和原理为导向，允许企业灵活地采取最合适于其的适当措施来解决此类风险问题。	We suggest changing Article 10 to the following: 我们建议对第 10 条修改如下： “**Article 10** When a data processor discovers that any network product or service it uses or provides has any security vulnerability or loophole, or poses any risk such as threatening national security or endangering public interests, such data

Article 条款	Comments 意见	Recommendation 建议
共利益等风险时，应当立即采取补救措施。		processor shall immediately take ~~remedial~~ appropriate measures. **第十条** 数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取适当~~补救~~措施。”
Article 11 A data processor shall establish an emergency response mechanism for data security incidents, promptly activate the emergency response mechanism in the event of a data security incident, and take measures to prevent the expansion of damage and eliminate potential security hazards. If a security incident causes any harm to an individual or organization, the data processor shall, within three business days, notify the interested parties by phone calls, SMS messages, instant messages or e-mails, of the security incident and the risks, the consequences of the harm and the remedial measures that have been taken, or inform them by public announcement if no notice is possible. If any law or administrative	Overall, data processors should have the ability to assess the severity of the security incident and determine on whether reporting is to be made to individuals or organizations taking into the level of risk of harm. 一般来说，数据处理者应当能够评估安全事件的严重性，并决定是否向个人或组织报告危害的风险水平。 In financial sector, there are existing requirements for financial institutions to report incidents to financial institutions' primary financial regulator. We recommend that the Regulations harmonize reporting requirements and allow financial institutions to report once to financial	We suggest changing Article 11 to the following: 我们建议对第 11 条修改如下： “**Article 11** A data processor shall establish an emergency response mechanism for data security incidents, promptly activate the emergency response mechanism in the event of a data security incident, and take measures to prevent the expansion of damage and eliminate potential security hazards. If a security incident causes any harm to an individual or organization, the data processor shall, within three business days, notify the interested parties by phone calls, SMS messages, instant messages or e-mails, of the security incident and the risks,

Article 条款	Comments 意见	Recommendation 建议
regulation permits the omission of notice, the data processor shall follow the provisions of such law or administrative regulation. If a security incident is suspected of constituting a crime, the data processor shall report the incident to the public security authority in accordance with relevant regulations. **第十一条** 数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患。安全事件对个人、组织造成危害的，数据处理者应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知，法律、行政法规规定可以不通知的从其规定。安全事件涉嫌犯罪的，数据处理者应当按规定向公安机关报案。 In the event of a data security incident such as the leakage, destruction or loss of	regulators who could coordinate with CAC further. When incident happens, firms need valuable resources for incident response and recovery, and requirements to report to multiple authorities would distract valuable resources from responding to an incident. 对于金融业，金融机构已经根据现有要求需要向金融监管机构报告安全事件。我们建议监管机构可以统一报告的要求，允许金融机构仅向金融监管机构提交报告，而金融监管机构可与贵办公室在安全报告方面进行更进一步的协调。我们认为，当安全事件发生时，企业需要宝贵的资源来应对事件并恢复秩序，而向多个监管机构报告的要求会分散企业宝贵的资源，从而阻碍对安全事件的及时响应。 We recommend that initial reporting of an incident can be provided through any form of written or oral communication (e.g., email or telephone), to a designated point of contact with a financial institution's primary	the consequences of the harm and the remedial measures that have been taken, or inform them by public announcement if no notice is possible. If any law or administrative regulation permits the omission of notice, the data processor shall follow the provisions of such law or administrative regulation. If a security incident is suspected of constituting a crime, the data processor shall report the incident to the public security authority in accordance with relevant regulations. **第十一条** 数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患。安全事件对个人、组织造成危害的，数据处理者应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知，法律、行政法规规定可以不通知的从其规定。安全事

Article 条款	Comments 意见	Recommendation 建议
important data, or personal information of 100,000 or more people, the data processor shall also perform the following obligations: 发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，数据处理者还应当履行以下义务： (1) within **eight hours** after the occurrence of the security incident, report basic information about the incident to the cyberspace authority and the relevant competent authorities at the districted city level, including the volume and type of the data involved, the possible impact, and the measures taken or to be taken to handle the incident; and （一）在发生安全事件的**八小时内**向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等； (2) within five business days after the handling of the incident is completed, it shall	regulator. During the first phase of incident response, financial institutions should be allowed to devote resources to response and mitigation and report updates to the primary regulator as necessary or as significant new information comes to light. Prescribing information that may be sent to regulators may challenge financial institutions to provide details that do not correspond to observable facts or analysis. This can lead to delays or the provision of inaccurate information. 我们建议，允许金融机构通过书面或口头沟通（如电子邮件或电话）的任何形式向金融监管机构的指定联系人进行安全事件的初始报告，并在必要时或发生新的重大数据泄露时向金融监管机构更新报告，原因是在应对安全事件的第一阶段，应允许金融机构将其资源用于安全事件的响应和缓解。此外明确规定需要报告给监管机构的内容可能会导致金融机构提供与	件涉嫌犯罪的，数据处理者应当按规定向公安机关报案。 In the event of a data security incident such as the leakage, destruction or loss of important data, or personal information of 100,000 or more people, the data processor shall also perform the following obligations: 发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，数据处理者还应当履行以下义务： (1) within ~~eight hours~~ 35 days commencing on the date on which the data processor becomes aware of the occurrence of the incident ~~after the occurrence of the security incident~~, report basic information about the incident to the ~~cyberspace authority and~~ the relevant competent authorities at the districted city level, competent authorities should further coordinate with cyberspace authority. ~~including the volume and type of the data involved, the possible impact, and~~

Article 条款	Comments 意见	Recommendation 建议
submit to the cyberspace authority and the relevant competent authorities at the districted city level an investigation and assessment report that includes but not limited to information about the cause of the incident, the consequences and impact, the punishment of those liable, and the improvement measures. （二）在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。	事实或分析不符的信息，从而可能导致报告的延迟或内容的不准确。 In terms of the reporting timeline, our members are of the view that the 8 hour time requirement is not practically feasible. In other jurisdictions, such as the United States, the time period for incident reporting allows for a 20 to 45 day period for such reporting to be effected. In practice, the immediate first priority of the data processor in the event of a data security incident is to mitigate the damage and prevent further data leakage, and to focus efforts on preventing further unauthorized access. There is also the risk that having reported in haste any proposed remediation action would result in ineffective measures being taken on the basis of insufficient information. 对于向监管机构进行报告的时间限制，我们的会员认为8小时的时间要求并不实际。在其他国家，如美国，允	~~the measures taken or to be taken to handle the incident~~; and （一）在数据处理者发现发生安全事件的~~八小时~~三十五日内向设区的市级~~网信部门和~~有关主管部门报告，有关主管部门应与网信部门积极协调~~事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等~~； (2) within 35~~five~~ business days after the handling of the incident is completed, it shall submit to the cyberspace authority and the relevant competent authorities at the districted city level an investigation and assessment report that includes but not limited to information about the cause of the incident, the consequences and impact, the punishment of those liable, and the improvement measures. （二）在事件处置完毕后三十五~~五~~个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、

Article 条款	Comments 意见	Recommendation 建议
	许 20 至 45 天的时间进行安全事件报告。我们认为，事实上，在发生数据安全事件时，数据处理者的第一要务是减轻损害和防范未来可能的数据泄漏，并集中精力防止进一步的未经授权访问。此外，匆忙地对任何拟采取的补救行动进行报告可能导致数据处理者在信息不全的情况下报告并采取无效的措施。 We noted the requirements for companies to submit an assessment report after the handling of the incident is completed, and would like to seek clarification on the definition of completion of incident handling. 我们注意到该条款要求企业在安全事件处置完毕后提交调查评估报告，我们希望贵办公室可以明确何为"事件处置完毕"。 In additions, the Regulations stipulate that reporting obligations commence on the	责任处理、改进措施等情况的调查评估报告。" Besides, for the notification requirement provided in Paragraph, the content of the notification shall include, amongst others, the remedial measures that have been taken - we would suggest CAC clarify that it does not intend to regulate that the processor shall accomplish all the measures but instead, it will suffice if the actions have been initiated to establish the remedial measures. 此外，对于第一款中规定的通知内容应包括"已经采取的处置措施"——我们建议贵办公室澄清，这里所指的处置措施并不要求数据处理者完成所有举措，只要数据处理者已经采取行动来实施补救，即满足该要求。

Article 条款	Comments 意见	Recommendation 建议
	date on which the incident occurs. This may not be practical given that not all incidents are discovered on a real time basis and may only be discovered after the fact. 此外，本条规定，报告义务从事件发生之日起算。我们认为这个要求可能不太实际，因为安全事件并非都可以立即实时被发现，可能只有在事后才能被发现。 Based on the above reasons, we respectfully suggest that a notification and reporting period of 35 days commencing on the date on which the data processor becomes aware of the occurrence of the incident. This would allow data processors the ability to focus on identifying and rectifying the incident in real time. 基于上述原因，我们诚恳地建议，将报告义务修改为在数据处理者发现事件之日起 35 天内，这也能促进数据处理者专注于实时识别和处理安全事件之中。	

Article 条款	Comments 意见	Recommendation 建议
Article 12 If a data processor provides personal information to any third party, or shares, trades, or entrusts the processing of, important data, the data processor shall: **第十二条** 数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规定： (1) inform the individuals concerned of the purpose, type, method and scope of its provision of personal information, and **the period and location of storage**, and obtain the individuals' separate consent, except in circumstances where no separate consent of individuals is required under laws or administrative regulations, or the information has been anonymized; （一）向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；	The Article should decouple PI and important data as the risk considerations for the two are different and the PIPL has laid down requirements for PI related data provision. 由于个人信息和重要数据的风险考虑因素不同，且《个人信息保护法》已规定了个人信息对外提供的要求，我们认为本条款不应将个人信息和重要数据混在一起进行规定。 For entrusted processing of PI, we recommend that the Regulations follow the requirements laid out in the PIPL where only cross-border data transfer needs separate consent from a PI subject and domestic sharing with 3rd party doesn't require separate consent. In addition, we recommend that CAC recognize that entrusted processing is different with data sharing and provision as entrusted processing doesn't involve the transfer of ownership of the data and control of the data is still with the data processor. For	The Article should decouple PI and important data. For PI, we recommend that the draft regulations follow and refer to the requirements laid out in the PIPL and not repeat and duplicate the requirements here – suggest to delete. For important data, the requirements shall not deviate from the general framework of the Laws. 本条应该将个人信息和重要数据分开规定。对于个人信息，我们建议本条例遵循并参考《个人信息保护法》中的规定，无需在本条中重复，因此建议删除。对重要数据的要求，我们认为不应偏离数据法律规定的总体框架。

Article 条款	Comments 意见	Recommendation 建议
(2) agree with the data recipient on the purpose, scope and method of data processing, and the data security protection measures, specify each party's responsibilities and obligations in relation to data security in a contract or other forms, and supervise the data recipient's data processing activities; and （二）与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督； (3) keep the records of personal consents, the log records of personal information provision, and keep the records and log records of the approval of the sharing, trading, or entrusted processing of, important data, for at least five years. （三）留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。	example, if an organization uses IaaS service, cloud service providers (CSPs) should not read and be allowed to read clients' data and differentiate data types (PI or non-PI or others) clients put on cloud and therefore should not be expected to engage with the PI subject. CSPs obligations as entrusted party should be defined by the PI processor. 对于个人信息的委托处理，我们建议本条例遵循《个人信息保护法》的规定，即只有提供涉及数据出境时才需要个人信息主体的单独同意，在国内委托处理不需要单独同意。此外，我们建议贵办公室明确委托处理与数据的共享和对外提供应当不同，因为委托处理不涉及数据控制权的转让，数据的控制权仍由委托方掌握。例如，如果一个组织使用基础设施即服务（IaaS）来为其客户提供服务，则云服务提供商不应读取，或被允许读取客户的数据，或区分客户上传至云端的数据类型（个人信息或非个人信息或	

Article 条款	Comments 意见	Recommendation 建议
The data recipient shall perform the agreed obligations and shall not process personal information or important data beyond the agreed purpose, scope, and method of processing. 数据接收方应当履行约定的义务，不得超出约定的目的、范围、处理方式处理个人信息和重要数据。	其他数据），因此云服务提供商并不是个人信息的处理者，其作为受托方，其义务应由作为个人信息处理者的委托方确定。 Besides, Article 12(2) expands the need to enter into a contract with a data recipient to recipients of 'important data' – there is no such provision right now under the DSL. 此外，第十二条第（二）项将需要与数据提供方签订协议的数据接收方的范围扩大到了"重要数据"的接收方，在《数据安全法》项下并没有此类规定。	
Article 13 A data processor shall apply for cyber security review in accordance with the relevant regulations of the State in order to: **第十三条** 数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查：	We seek clarification on Article 13(3) – what industries or businesses would be viewed for its listing in HK which affects or may affect national security and the interpretation of "may affect national security". 我们希望贵办公室可以进一步解释第十三条第（三）项规定的情形，哪些行业或企业在香港上市会影响或可能	

Article 条款	Comments 意见	Recommendation 建议
(1) as an Internet platform operator that gathers and masters a large amount of data resources concerning national security, economic development and public interests, implement a merger, reorganization or division that affects or may affect national security; （一）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的； (2) as a data processor that processes personal information of one million or more people, be listed abroad; （二）处理一百万人以上个人信息的数据处理者赴国外上市的； (3) be listed in Hong Kong Special Administrative Region, if the listing affects or may affect national security; or （三）数据处理者赴香港上市，影响或者可能影响国家安全的；	影响国家安全，以及“可能影响国家安全”的含义。 As mentioned in Section 1.2, we also suggest CAC to clarify how the 1 million threshold should be calculated for Article 13(2). 如正文第 1.2 节所述，我们还建议贵办公室明确第（二）项的一百万应当如何计算。	

Article 条款	Comments 意见	Recommendation 建议
(4) conduct any other data processing activity that affects or may affect national security. （四）其他影响或者可能影响国家安全的数据处理活动。 To set up a headquarters or an operation center or research and development center abroad, a large Internet platform operator shall submit a report to the national cyberspace authority and the competent authorities. 大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。		
Article 14 If a data processor experiences a merger, reorganization or division, the data recipient shall continue to perform the data security protection obligations and, if important data or the personal information of one million or more people is involved, it shall submit a report to the competent authorities at the districted city level. If a data processor is dissolved or declared bankrupt, it shall submit a report to	Data processors should be given the prerogative to set out their policies and procedures pertaining to the processing of data, including the data's lifecycle, instead of being required to handover its data to the authorities. 我们认为数据处理者应有权制定与数据处理相关的政策和流程，包括数据	We recommend that the Article be deleted. If the Article is to be retained, we recommend that the Regulations align with existing sectoral rules and not prescribe further obligations for financial sector. 我们建议删除本条。如果本条还是会被保留，我们希望本条例可以与现有的行

Article 条款	Comments 意见	Recommendation 建议
the competent authorities at the districted city level, hand over or delete the data in accordance with relevant requirements or, if the competent authorities is not clear, it shall submit a report to the cyberspace authority at the districted city level. **第十四条**　数据处理者发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告；数据处理者发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。	的生命周期，而不是被要求将数据移交给主管部门。 Our members feel that the general description of mergers, reorganizations and divisions is ambiguous and would suggest that the corporate transactions that would trigger the application of this Article 14 be clearly specified. 我们的会员认为，该条款对合并、重组和分立的规定较为模糊，建议对适用第 14 条的公司交易进行明确。 For example, restructurings, reorganizations or divisions could potentially capture a broad range of ordinary course corporate transactions (e.g. asset sales, changing the type of entity, intercompany transfers of assets or division of functions in the ordinary course of business). Typically, global financial groups engage in internal "restructurings" of their operations and functions on a frequent basis (which may be major or minor in	业规定一致，不对金融机构施加额外的义务。 Besides, we would therefore suggest that CAC provide limit the scope to restructurings where the actual controller of the data processor is changed, or at least provide certain carve-outs for ordinary course corporate transactions if it is not the intention to capture such acts. 此外，我们进一步建议贵办公室可以对"重组"的范围进行限缩，即只有数据处理者的实际控制人变更才构成"重组"，或者至少排除正常经营过程中的公司交易行为（如果贵办公室设置本条的本意并不涵盖此类行为）。 In addition, we would suggest the CAC to clarify that the reporting obligation is not intended to be an approval requirement but more a filing.

Article 条款	Comments 意见	Recommendation 建议
	nature) and it is not clear from the regulations what types of "restructurings" would be considered to trigger the reporting obligation. 例如，该条款规定的重组或分立可能会将大范围的公司正常经营过程中的交易类型（例如，资产出售、公司组织形式变更、资产转移或正常经营过程中的部门拆分）包括进去。全球金融集团经常对其运营和职能部门进行内部"重组"（可能重大，也可能不重大），而该规定没有明确哪些类型的"重组"将触发报告义务。 Besides, in financial sector, there are existing requirements for financial institutions to report M&A, restructuring or spin-off activities to financial regulators. 此外，金融业已有规定要求金融机构将其兼并收购、重组或分立的行为向金融监管部门进行报告。	此外，我们建议贵办公室明确本条规定的报告义务并不构成事先审批的要求，而是一种事后备案的义务。
Article 15 The data processor shall fulfill their data security protection	The requirement set out in this Article15 is not practical or reasonable. For example, if	We suggest this Article be removed for the wording is broad and vague. If this Article is

Article 条款	Comments 意见	Recommendation 建议
obligations in accordance with the provisions of the Regulations when obtaining data from other sources. **第十五条** 数据处理者从其他途径获取的数据，应当按照本条例的规定履行数据安全保护义务。	a financial institution receives IPO due diligence reports that relate to a company and generate important data, the financial institution will be subject to all applicable requirements in relation to important data, such as compiling and filing an annual report. 第 15 条规定的要求并不现实，或者说欠缺合理性。例如，如果一个金融机构接收到有关一个公司首次公开发行的尽职调查报告，其中包括重要数据，那么根据该第 15 条的规定，这一金融机构将适用有关重要数据的所有要求，例如编制并报送年度报告。	to be retained, we suggest CAC provide more pre-conditions, parameters to ensure the implementation and avoid misunderstanding. 由于本条的表述外延广泛且语意不明，我们建议删除本条。若仍然保留，我们建议贵办公室可以进一步规定一些前提条件或要件以确保条款的可执行性，且避免误解。
Article 17 When using an automated tool to access or collect data, a data processor shall assess the impact on the performance and functions of network services, and shall not interfere with the normal functions of network services. **第十七条** 数据处理者在采用自动化工具访问、收集数据时，应当评估对网	We strongly recommend that the draft Regulations recognize that industry self-discipline convention are market driven and voluntary and should not be mandated to all companies. 我们强烈建议本条例承认行业自律公约是市场导向且自愿遵守的，不应对所有公司强制适用。	We suggest changing Article 17 to the following: 我们建议对第 17 条修改如下： **"Article 17** When using an automated tool to access or collect data, a data processor shall assess the impact on the performance and functions of network services, and shall not interfere with the normal functions of network services.

Article 条款	Comments 意见	Recommendation 建议
络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。 If a data processor's use of an automated tool to access or collect data violates any law, administrative regulation, or industry self-discipline convention, affects the normal functions of network services, or infringes upon the intellectual property right or other legal rights or interests of another person, the data processor shall stop the data access or collection and take corresponding remedial measures. 自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行为并采取相应补救措施。	Mandatory obligations for firms should be clearly laid out in laws and regulations. 对公司适用的强制性义务应当在法律法规中明确。	**第十七条** 数据处理者在采用自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。 If a data processor's use of an automated tool to access or collect data violates any law, administrative regulation, ~~or industry self-discipline convention~~, affects the normal functions of network services, or infringes upon the intellectual property right or other legal rights or interests of another person, the data processor shall stop the data access or collection and take corresponding remedial measures. 自动化工具访问、收集数据违反法律、行政法规~~或者行业自律公约~~、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行为并采取相应补救措施。"

Article 条款	Comments 意见	Recommendation 建议
Article 18 A data processor shall establish a convenient channel for receiving data security complaints and whistleblowing reports, and accept and address such complaints and reports in a timely manner. **第十八条** 数据处理者应当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。 A data processor shall publish its contact details for accepting complaints and whistleblowing reports, and information about the person responsible therefor, and shall publicly disclose on an annual basis the number of personal information security complaints accepted and received, the addressing of such complaints, and the average period used for addressing such a complaint for the public to supervise. 数据处理者应当公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。	The requirement to set up customer service channels for PI related questions and complaints should only apply to PI processors. 对个人信息有关问题和投诉建立客服渠道的要求应当仅适用于个人信息处理者。 For important data, it is our understanding that organizations with important data should not publicly share that they own important data. Therefore, it doesn't make sense to set up public channel and be subject to public supervision. 对于重要数据，我们理解持有重要数据的机构不应公开发布其所有的重要数据，因此设置公开披露渠道以及接收社会监督的规定对其没有意义。 We recommend that CAC align approaches with global practice, such as GDPR, in dealing with PI related complaints or issues and not require disclosure of complaints and complaints handling.	We suggest removal of disclosure of PI related complaints and public supervision and changing the Article to the following: 我们建议删除个人信息相关投诉的披露和接受社会监督的要求，并建议将本条修改如下： "**Article 18** A PI ~~data~~ processor shall establish a convenient channel for receiving ~~data~~ PI security complaints and whistleblowing reports, and accept and address such complaints and reports in a timely manner. **第十八条** 个人信息~~数据~~处理者应当建立便捷的个人信息~~数据~~安全投诉举报渠道，及时受理、处置数据安全投诉举报。 A PI ~~data~~ processor shall publish its contact details for accepting complaints and whistleblowing reports, and information about the person responsible therefor~~, and shall publicly disclose on an annual basis the~~

Article 条款	Comments 意见	Recommendation 建议
	在个人信息投诉或问题处理方面，我们建议贵办公室可以遵照国际实践，例如 GDPR，并且不应要求对此类投诉和投诉处理情况进行公开披露。 The Regulations should align with requirements from sectoral regulators, who should be in charge of sector's overall compliance. For example, the banking sector has already established the annual information disclosure regime and it is more reasonable and efficient to include the disclosure contents as required in Article 18 in the banking annual disclosure so that the banking institutions may not need to prepare separate disclosure documents. 本条例也应当与负责监管整个行业合规问题的行业监管部门的要求保持一致。例如，银行业已经建立了年度信息披露制度，将此第 18 条规定的披露内容纳入银行年度信披报告中会更加合理和高效，这样银行业机构无需再准备单独的信息披露文件。	~~number of personal information security complaints accepted and received, the addressing of such complaints, and the average period used for addressing such a complaint for the public to supervise~~. 个人信息~~数据~~处理者应当公布接受投诉、举报的联系方式、责任人信息~~，每年公开披露受理和收到的个人信息安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督~~。”

Article 条款	Comments 意见	Recommendation 建议
Chapter 3 Personal Information Protection **第三章 个人信息保护**		This Chapter overlaps and duplicates with the requirements under the PRC PIPL. Propose that this be deleted. It is not necessary to repeat these requirements here. 本章与《个人信息保护法》的要求存在重复。重复规定是不必要的，建议删除。
Article 19 A data processor's processing of personal information shall be for a clear and reasonable purpose, and follow the principles of lawfulness, justifiability, and necessity. The processing of personal information based on an individual's consent shall meet the following requirements: **第十九条** 数据处理者处理个人信息，应当具有明确、合理的目的，遵循合法、正当、必要的原则。基于个人同意处理个人信息的，应当满足以下要求： (1) the personal information processed is necessary for providing the service, or for performing obligations under any law or administrative regulation;	We suggest that the Regulations allow firms the flexibility to determine what constitutes "necessary" processing of PI for service provision based on its own handling process and risk tolerance. 我们建议本条例应允许企业根据自身的处理流程和风险承受能力，自主决定提供服务所"必需"的个人信息。	We suggest deleting Article 19(1). 我们建议删除第 19 条第一款第(一)项。

Article 条款	Comments 意见	Recommendation 建议
（一）处理的个人信息是提供服务所必需的，或者是履行法律、行政法规规定的义务所必需的； (2) the processing is limited to the shortest period and the lowest frequency required for achieving the purpose of the processing, and conducted in a manner that has the least impact on the individual's rights and interests; and （二）限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式； (3) the data processor shall not refuse to provide the service or interfere with the individual's normal use of the service due to the individual's refusal to provide information other than that necessary for providing services. （三）不得因个人拒绝提供服务必需的个人信息以外的信息，拒绝提供服务或者干扰个人正常使用服务。		

Article 条款	Comments 意见	Recommendation 建议
Article 20 When processing personal information, the data processor shall formulate policies for the processing of personal information and strictly abide by them. The policies for the processing of personal information shall be displayed in a centralized and public manner, shall be easily accessible and placed in a prominent position, shall provide with clear, specific, concise and reader-friendly contents and a systematic and comprehensive description of the processing of personal information to individuals. **第二十条** 数据处理者处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。 Personal information processing policies shall include but not limited to the following:	The Regulations provide for higher or brand new requirements of the content in such policy, as compared with other rules or industrial standards. For example, Article 20(2) adds a requirement to specify term of storage and method of processing after expiration – both of which are new requirements. 与其他规则或行业标准相比，本条例对个人信息处理规则的内容提出了更高的或新的要求。例如，第 20 条第一款第（二）项要求在个人信息处理规则中明确存储期限和到期后的处理方法——这两项都是新增的要求。 Article 20(1) seems to suggest that there will be individual 'product' or 'service' aligned consents and from perspective of financial institutions, this is going to be very onerous for those that provide a suite of products and services and would likely to result in much less impactful consents if followed as drafted.	We advocate CAC re-consider the practical feasibility in imposing such strict standard and align the requirements with published rules/standards and market practice. 我们建议贵办公室对该等严格要求的实际可行性进行重新考虑，并将此类要求进行调整以符合已发布的规则/标准和市场实践。 We also suggest clarifying that the "third party" referred in Article 20(4) only applies to external third parties and doesn't include intra-group affiliates. As an example, a MNC's HQ may centrally provide IT support to multiple entities in various jurisdictions and the entities within the same group share the same controls, which should not be covered under "third party" reference here. 我们还建议将第 20 条第一款第（四）项中的"第三方"明确为仅适用于外部第三方，不包括集团内的关联公司。例如，跨国公司的总部可能会集中向不同

Article 条款	Comments 意见	Recommendation 建议
个人信息处理规则应当包括但不限于以下内容： (1) specifying the personal information required in accordance with the functions of the product or service, providing the purpose, usage, method, type, frequency or timing of personal information processing, the place of storage, etc. in a list format, and the impact of refusal to process personal information on individuals; （一）依据产品或者服务的功能明确所需的个人信息，以清单形式列明每项功能处理个人信息的目的、用途、方式、种类、频次或者时机、保存地点等，以及拒绝处理个人信息对个人的影响； (2) providing the period of personal information storage or the determination method of the period of personal information storage, and the method of processing after expiration;	第 20 条第一款第（一）项似乎表明个人同意应当基于每项“产品”或“服务”作出，从金融机构的角度来看，这项规定对于提供一整套产品和服务的金融机构而言会导致繁重的义务，并且如果按照目前起草的规定执行，其所取得的同意的有效性会减小。	司法管辖区的多个实体提供信息技术支持，由于同一集团内的多个实体的实际控制人相同，这种情况不应属于“第三方”。

Article 条款	Comments 意见	Recommendation 建议
（二）个人信息存储期限或者个人信息存储期限的确定方法、到期后的处理方式； (3) providing the ways and methods for individuals to access, copy, correct, delete, restrict the processing of and transfer personal information, as well as to cancel accounts and withdraw consent to personal information processing; （三）个人查阅、复制、更正、删除、限制处理、转移个人信息，以及注销账号、撤回处理个人信息同意的途径和方法； (4) explaining all third-party codes and plug-ins embedded in the product services to collect personal information in a way that facilitates user's access, such as centralized display, as well as the purpose, method, type, frequency or timing of the collection of personal information by each **third-party** code or plug-in and the rules governing the processing of personal information;		

Article 条款	Comments 意见	Recommendation 建议
（四）以集中展示等便利用户访问的方式说明产品服务中嵌入的所有收集个人信息的第三方代码、插件的名称，以及每个第三方代码、插件收集个人信息的目的、方式、种类、频次或者时机及其个人信息处理规则； (5) specifying the circumstances in which personal information is provided to third parties and its purpose, method, type, information about the data recipient, etc.; （五）向第三方提供个人信息情形及其目的、方式、种类，数据接收方相关信息等； (6) providing personal information security risks and protective measures; （六）个人信息安全风险及保护措施； (7) providing complaints and reporting channels and methods of resolution of personal information security issues, contact		

Article 条款	Comments 意见	Recommendation 建议
information of the persons responsible for personal information protection. （七）个人信息安全问题的投诉、举报渠道及解决途径，个人信息保护负责人联系方式。		
Article 21 Where consent shall be obtained from the individuals to process the personal information, data processors shall abide by the following provisions: **第二十一条** 处理个人信息应当取得个人同意的，数据处理者应当遵守以下规定： (1) applying to individuals for their consents respectively to process personal information according to the type of service, and may not obtain consent using general terms; （一）按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意； (2) obtaining individual's separate consent to process sensitive personal information such	The requirements for obtaining the consent are onerous and we seek CAC's clarification re the following points: 取得同意的要求对个人信息处理者较为繁重，我们希望贵办公室可以对以下几点进行澄清： (1) consents shall be obtained based on the "types of services" respectively – does it mean the consent should be obtained at service level rather than PI processing level, the latter of which is in line with the processing activities mentioned in the PIPL; 按照"服务类型"分别向个人申请处理个人信息的同意——是否意味着对于征求同意的要求，个人信息处理者应在服务层面征求同意，而不	We suggest the CAC clarify Article 21 only applies when consent is relied on as the lawful basis. Therefore, we suggest changing the Article to the following: 我们建议贵办公室对第 21 条明确仅适用于以个人同意作为个人信息处理的合法依据的情形。因此，我们建议将本条修改为： "**Article 21** Where consent is relied on as the lawful basis ~~shall be obtained from the individuals~~ to process ~~the~~ individuals' personal information, data processors shall abide by the following provisions: **第二十一条** 处理个人信息以个人同意作为合法依据的~~应当取得个人同意的~~，数据处理者应当遵守以下规定：

Article 条款	Comments 意见	Recommendation 建议
as biometric identification, religious beliefs, specific identities, medical health, financial accounts, whereabouts and tracks; （二）处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意； (3) obtaining the consent from his/her guardian to process the personal information of a minor under the age of fourteen; （三）处理不满十四周岁未成年人的个人信息，应当取得其监护人同意； (4) not forcing the individual to give consent to the processing of personal information on the grounds of improving service quality, enhancing user experience, developing new products, etc.; （四）不得以改善服务质量、提升用户体验、研发新产品等为由，强迫个人同意处理其个人信息；	是根据《个人信息保护法》规定的对个人信息处理活动征求同意； (2) in addition to (1), does the requirement mean each business line or specific service? E.g. private banking/private wealth management vs distribution + advisory + trade execution + etc.; 除第(1)点外，该要求是适用于所有业务线还是特定服务？例如，私人银行/私人财富管理 vs 销售+咨询+交易执行等业务； (3) every time there is change to the processing arrangements in relation to personal information, the processer shall re-obtain the consent and in the meantime, update the policy – this is new requirement in addition to the PIPL. It is suggested that the CAC provide clearer time limit/sequence for the two steps, instead of using the broad term "in the meantime". 每当个人信息处理安排发生变化，处理者都应重新取得同意，并同步	(1) applying to individuals for their consents respectively to process personal information according to the type of service, and may not obtain consent using general terms; （一）按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意； (2) obtaining individual's separate consent to process their personal information (including sensitive personal information) where required by the Personal Information Protection Law ~~such as biometric identification, religious beliefs, specific identities, medical health, financial accounts, whereabouts and tracks~~;…" （二）处理~~个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等~~个人信息（包括敏感个人信息）应当根据《个人信息保护法》的要求取得个人单独同意；……" Besides, we suggest CAC consider our comments and make additional and

Article 条款	Comments 意见	Recommendation 建议
(5) not obtaining the consent through misleading, fraudulent or coercive means; （五）不得通过误导、欺诈、胁迫等方式获得个人的同意； (6) not inducing or compelling the individual to consent to bulk personal information by bundling different types of services or applying for consent in bulk; （六）不得通过捆绑不同类型服务、批量申请同意等方式诱导、强迫个人进行批量个人信息同意； (7) not processing the personal information beyond the scope of the consent authorized by the individual; （七）不得超出个人授权同意的范围处理个人信息； (8) not soliciting consent frequently or interfering with the normal use of the services after the individual expressly disagrees.	修改个人信息处理规则——这是《个人信息保护法》之外的新要求。我们建议贵办公室为这两个步骤提供更明确的时间限制/顺序要求，而非"同步"这一宽泛的表述。	necessary revisions to proposed Article 21 above. 此外，我们建议贵办公室考虑我们的其他意见，并对上述我们提议的第 21 条作出进一步的必要修订。

Article 条款	Comments 意见	Recommendation 建议
（八）不得在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。 If there is a change in the purpose, mode and type of personal information processed for the processing of personal information, data processors shall obtain the consent of the individual concerned anew and modify the policies for the processing of personal information simultaneously. 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。 Where the validity of an individual's consent is in dispute, the data processor bears the burden of proof. 对个人同意行为有效性存在争议的，数据处理者负有举证责任。		
Article 22 Under any of the following circumstances, a data processor shall delete the personal information or anonymize it within fifteen business days:	15 business days is too tight a timeframe for deletion of data and likely to drive most organisations to relying upon the 'technically difficult' exception (making it	We suggest extending the requirement of 15 business days to 30 business days.

Article 条款	Comments 意见	Recommendation 建议
第二十二条 有下列情况之一的，数据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理： (1) where the purpose of processing personal information has been achieved or it is no longer necessary to achieve the purpose of processing personal information; （一）已实现个人信息处理目的或者实现处理目的不再必要； (2) where the storage period agreed with the user or clearly defined by the rules for the processing of personal information has expired; （二）达到与用户约定或者个人信息处理规则明确的存储期限； (3) where the service has been terminated or the individual's account has been cancelled; （三）终止服务或者个人注销账号； (4) where non-essential personal information or personal information without the consent	operate more as a rule than an exception) and the associated explanation to the individuals. 在十五个工作日内删除数据的时间要求太过紧迫，可能会促使大多数机构依赖"技术上难以实现"的豁免情形（从而导致"技术上难以实现"这一例外情形变成通用规则）并对个人作出有关解释。 The definition and type of "necessary security protection measures" under the second paragraph remains unclear, which should be clarified by providing practical guidance for data processors. 第二款中"必要的安全保护措施"的定义和类型尚不明确，建议为数据处理者提供实践指引进行澄清。 Besides, these destruction periods are unrealistic for large MNCs particularly regulated financial institutions with obligations to retain archives for years. Even for smaller companies records of data	我们建议将十五个工作日的要求延长至三十个工作日。 Besides, we suggest changing the first paragraph of Article 22 to the following: 此外，我们建议将第 22 条第一款修改如下： "**Article 22** Under any of the following circumstances, an individual shall have the right to request the data processor to delete or anonymize the personal information and the data processor shall consent to and proceed with such request as long as such request is not in violation of other laws or rules, or the individual has provided with reasonable explanation: ...~~data processor shall delete the personal information or anonymize it within fifteen business days:~~" **第二十二条** 有下列情况之一的，~~数据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理：~~个人有权要求数据处理者删除个人信息或者进行匿名化处理，但该请求不得违反其他法律

Article 条款	Comments 意见	Recommendation 建议
of individuals has been inevitably collected due to the use of automated data collection technology. （四）因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息。 If it is technically difficult to delete personal information, or it is difficult to delete personal information within fifteen business days due to business complexity, data processors shall not carry out processing other than storage and taking necessary security protection measures, and shall give reasonable explanation to individuals. 删除个人信息从技术上难以实现，或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要的安全保护措施之外的处理，并应当向个人作出合理解释。	would need to be retained for at least as long as needed to defend themselves in claims so at least align with limitation periods. 此外，该删除期限对于大型跨国企业来说是不现实的，特别是受监管的金融机构承担着在相应年数期限内留存档案的义务。即使对于小型企业，当其被索赔时，出于为自己进行辩护的目的，也至少需要在诉讼时效内保留数据记录。	法规，除非个人已提供以下合理解释：……” Since the financial regulators have specific requirements on the retention period for customers' PI under regulations and regulatory circulars, which are not regarded as laws and administrative regulations under PRC legal regime, we recommend adding "regulatory requirements from industry regulators" into the last paragraph. 由于金融监管机构在部门规章和监管通知中对金融机构的客户个人信息的保留期限有具体要求，该等规则在中国法律制度下不属于法律和行政法规，我们建议在本条最后一款添加“行业监管部门的监管要求”。

Article 条款	Comments 意见	Recommendation 建议
Where laws and administrative regulations provide otherwise, such provisions shall prevail. 法律、行政法规另有规定的从其规定。		
Article 23 Where an individual makes a reasonable request to access, copy, correct, supplement or delete his personal information or restrict the processing of his personal information, data processors shall perform the following obligations: **第二十三条** 个人提出查阅、复制、更正、补充、限制处理、删除其个人信息的合理请求的，数据处理者应当履行以下义务： (1) providing convenient methods and ways to support for personal structured inquiries on the type and quantity of the collected personal information and etc., and may not limit the reasonable request of individuals by time, location and other factors; （一）提供便捷的支持个人结构化查询本人被收集的个人信息类型、数量等的	It would be helpful if the CAC clarified what is meant by 'makes a reasonable request' under this Article with respect to access, copy, correction, supplement or delete PI requests as it's quite vague as drafted and noting refusals provides the individual with a private right of action where fault is assumed to be on the part of the data processor unless they can prove otherwise, the consequence for misunderstanding has the potential to be significant. 我们希望贵办公室可以澄清本条中关于查阅、复制、更正、补充、限制处理、删除个人信息的"合理请求"的具体含义，因为"合理请求"这一用语较为模糊。我们还注意到，数据处理者拒绝该请求将导致个人有权采取行动，除非数据处理者能够提供相反证	We recommend CAC provide more elaboration on "makes a reasonable request" and we suggest bullet (3) shall be revised as follows: 我们建议贵办公室可以进一步解释"合理请求"的含义，同时我们希望对第（三）项作出如下修改： "(3) ~~processing and~~ giving feedback within thirty ~~fifteen~~ business days after the receipt of an individual's application to copy, correct, supplement or delete its personal information, restrict the processing of its personal information, withdraw authorized consent or cancel its account. Such thirty-day requirement may be extended to sixty-day taking into account the complexity and number of requests, provided the individual concerned is informed of such extension

Article 条款	Comments 意见	Recommendation 建议
方法和途径，不得以时间、位置等因素对个人的合理请求进行限制； (2) providing convenient functions to support for individuals to copy, correct, supplement or delete their personal information, or restrict processing of their personal information, or withdraw their authorized consent or cancel their accounts, and may not set unreasonable conditions; （二）提供便捷的支持个人复制、更正、补充、限制处理、删除其个人信息、撤回授权同意以及注销账号的功能，且不得设置不合理条件； (3) processing and giving feedback within fifteen business days after the receipt of an individual's application to copy, correct, supplement or delete its personal information, restrict the processing of its personal information, withdraw authorized consent or cancel its account. （三）收到个人复制、更正、补充、限制处理、删除本人个人信息、撤回授权	据，否则将被推定为存在过错，因此如果数据处理者不理解"合理请求"的含义，造成的后果可能会较为严重。 The 15 business day timeframe to process the requests is also quite tight under bullet (3), and doesn't seem to allow for an extension if required. 本条第（三）项规定的十五个工作日的处理时间要求也较为紧迫，而且本条似乎也不允许在必要情况下的延期。	within 30 days upon receipt of the request along with reasons for the delay. （三）收到个人复制、更正、补充、限制处理、删除本人个人信息、撤回授权同意或者注销账号申请的，应当在三十~~十五~~个工作日内~~处理并~~反馈。数据处理者可根据申请的复杂程度和数量将上述三十个工作日延长到六十个工作日，但数据处理者应当在收到个人申请后三十日内将上述延长告知有关个人，并说明原因。"

Article 条款	Comments 意见	Recommendation 建议
同意或者注销账号申请的，应当在十五个工作日内处理并反馈。 Where laws and administrative regulations provide otherwise, such provisions shall prevail. 法律、行政法规另有规定的从其规定。		
Article 24 Where the requests for the transfer of personal information that meet the following conditions, data processors shall provide transfer services for other data processors designated by the individual to access and obtain his/her personal information: **第二十四条** 符合下列条件的个人信息转移请求，数据处理者应当为个人指定的其他数据处理者访问、获取其个人信息提供转移服务： (1) the personal information requested for transfer is personal information collected on the basis of consent or necessary to enter into or perform the contracts;	In terms of the risk warning requirement, it is practically impossible to expect the data processor to assess the likelihood that the recipient to whom the data subject is asking the data processor to transfer their PI may/may not process that PI illegally, particularly where the recipient operates in a differing industry to the data processor - the data processor's employee processing the request may not recognise any red flags that pop up during the processing of the transfer request for what they are (even if another employee may due to their differing experience/background/role). The onus ought to be on the data subject rather than the data processor to perform due diligence	We recommend the risk warning requirement shall be removed. 我们建议删除风险提示的要求。

Article 条款	Comments 意见	Recommendation 建议
（一）请求转移的个人信息是基于同意或者订立、履行合同所必需而收集的个人信息； (2) the personal information requested for transfer is the personal information of the individual or information of others that the requester has legally obtained and does not go against the will of others; （二）请求转移的个人信息是本人信息或者请求人合法获得且不违背他人意愿的他人信息； (3) the legal identity of the requester can be verified. （三）能够验证请求人的合法身份。 If a data processor discovers that other data processors receiving personal information are at risk of illegally processing personal information, it shall make reasonable risk warnings for the transfer request of personal information.	on the recipient to whom they are directing the data processor to transfer their PI. 就风险提示要求而言，实际上数据处理者无法评估数据接收者是否具有非法处理个人信息的可能性，尤其是当接收者与数据处理者处于不同的行业时 – 处理转移请求的数据处理者的员工可能无法识别在处理转移请求期间出现的任何风险信号（即使另一名员工可能由于其不同经验/背景/角色而可以识别）。我们认为应由数据主体自身对其提出的转移个人信息请求而接收其个人信息的接收者进行尽职调查，而不是由根据数据主体的请求而进行数据转移的数据处理者进行该等尽职调查。	

Article 条款	Comments 意见	Recommendation 建议
数据处理者发现接收个人信息的其他数据处理者有非法处理个人信息风险的，应当对个人信息转移请求做合理的风险提示。 If the number of requests for the transfer of personal information is significantly beyond a reasonable range, data processors may charge a reasonable fee. 请求转移个人信息次数明显超出合理范围的，数据处理者可以收取合理费用。		
Article 26 A data processor processing personal information of one million or more people shall also comply with the provisions on the processors of important data set forth in Chapter 4 of these Regulations. **第二十六条** 数据处理者处理一百万人以上个人信息的，还应当遵守本条例第四章对重要数据的处理者作出的规定。	Similar to our comments in Section 1.2(3) and Section 2.2, volume itself is not a meaningful indicator of risk given the differences that exist between various categories of PI. Internationally, PI protection is for reasons such as privacy protection and personal interests and has no connection with national security. Grouping PI with national security data is not compatible with global norms and the spirit in multi-lateral agreements such as CPTPP, RCEP and DEPA.	We recommend that the draft Regulations decouple PI and important data and remove Article 26. 我们建议本条例不应将个人信息和重要数据混合规定，并删除第 26 条。

Article 条款	Comments 意见	Recommendation 建议
	正如我们在本文第 1.2(3)节和第 2.2 节的意见所述，鉴于各种类别的个人信息之间存在差异，处理个人信息的数量本身并不是一个对风险评估有意义的指标。在国际上，对个人信息的保护是出于隐私保护和个人利益等原因，与国家安全无关。将个人信息与国家安全数据打包的做法与国际惯例存在出入，也与多边协议（例如 CPTPP、RCEP 以及 DEPA）的精神违背。	
Article 27 All regions and departments shall, in accordance with the relevant requirements and standards of the State, organize data processors in different regions, departments and related industries and fields to identify important data and core data, organize the formulation of catalogues of important data and core data in their regions, departments and related industries and fields, and report the results to the Cyberspace Administration of China. **第二十七条** 各地区、各部门按照国家有关要求和标准，组织本地区、本部门	We would like to understand what would be contemplated in relation to the financial sector, as we believe that it would be rather disruptive to have different definitions and categories of important data apply in different regions of the PRC or for such categories to differ from department to department if there is more than one department that would have regulatory oversight over the financial sector in this regard. 我们希望知悉与金融行业有关的安排，因为我们认为如果中国不同地区	

Article 条款	Comments 意见	Recommendation 建议
以及相关行业、领域的数据处理者识别重要数据和核心数据，组织制定本地区、本部门以及相关行业、领域重要数据和核心数据目录，并报国家网信部门。	适用不同的重要数据定义和分类，或者如果有一个以上的部门在这方面对金融行业有监管权，而该等分类在不同部门间存在差别，那么将会造成一定的混乱。	
Article 28 The processor of important data shall clearly identify the person in charge of data security and set up a data security management department. The data security management department, under the leadership of the person in charge of data security, performs the following responsibilities: **第二十八条** 重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责： (1) Researching and making recommendations for major decisions related to data security;	We note that the DSL and PIPL seem to require data processors to hire two individuals to be in charge of data security and PI protection respectively. We recommend the CAC clarify in the Regulations that it is sufficient to hire one person to be responsible for both functions (to the extent the expertise of the relevant individuals support such setup, and the data processors so desire) given substantive overlapping between the two functions. 我们注意到《数据安全法》和《个人信息保护法》分别要求数据处理者聘请两名自然人以负责数据安全和个人信息保护。鉴于以上两种职能之间的实质性重叠，我们建议贵办公室在本条例中澄清聘请一人同时负责这两项职能即可（在相关人员的专业能力足	We suggest Article 28 shall be changed as follows: 我们建议第 28 条可以修改如下： "**Article 28** The processor of important data shall clearly identify the person in charge of data security and set up a data security management department. The data security management department, under the leadership of the person in charge of data security, performs the following responsibilities: **第二十八条** 重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：

Article 条款	Comments 意见	Recommendation 建议
（一）研究提出数据安全相关重大决策建议； (2) Formulating and implementing a data security protection plan and an emergency plan for data security incidents; （二）制定实施数据安全保护计划和数据安全事件应急预案； (3) Carrying out data security risk monitoring and timely dispose of data security risks and incidents; （三）开展数据安全风险监测，及时处置数据安全风险和事件； (4) Regularly organizing and carrying out data security publicity and education training, risk assessment, emergency drills and other activities; （四）定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动； (5) Accepting and handling data security complaints and reports;	够支持这种安排，且数据处理者也希望作此类安排的情况下）。 In particular, we note that financial institutions are subject to regulatory requirements on senior management personnel (SMP) and the qualifications of such SMPs, as well as the number and positions of such SMPs. Given that Article 28 of the Regulations require the responsible person in charge of data security to be in a position at a "decision-making level", we recommend that this position can be either an SMP or under the supervision of an SMP – we would appreciate it if the regulator can give more flexibility. 特别是，我们注意到，金融机构须遵守对高级管理人员的监管要求，以及对高级管理人员的任职资格、数量和职位要求。鉴于本条例第 28 条要求数据安全负责人应当是一个"决策层"职位，我们建议该职位可以是高级管理	(1) Researching and making recommendations for major decisions related to data security; （一）研究提出数据安全相关重大决策建议； (2) Formulating and implementing a data security protection plan and an emergency plan for data security incidents; （二）制定实施数据安全保护计划和数据安全事件应急预案； (3) Carrying out data security risk monitoring and timely dispose of data security risks and incidents; （三）开展数据安全风险监测，及时处置数据安全风险和事件； (4) Regularly organizing and carrying out data security publicity and education training, risk assessment, emergency drills and other activities;

Article 条款	Comments 意见	Recommendation 建议
（五）受理、处置数据安全投诉、举报； (6) Reporting the data security situation to the cyberspace administration and the competent and regulatory authorities in a timely manner as required. （六）按照要求及时向网信部门和主管、监管部门报告数据安全情况。 The person in charge of data security shall have the expertise of data security and relevant management working experience, be undertaken by the decision-making level members of the data processor, and shall have the right to report the data security situation directly to the cyberspace administration and the competent and regulatory authorities. 数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。	职位或受高级管理人员监督，我们期待监管机构能给予更多灵活性。	（四）定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动； (5) Accepting and handling data security complaints and reports; （五）受理、处置数据安全投诉、举报； (6) Reporting the data security situation to the cyberspace administration and the competent and regulatory authorities in a timely manner as required. （六）按照要求及时向网信部门和主管、监管部门报告数据安全情况。 The person in charge of data security shall have the expertise of data security and relevant management working experience, be undertaken by the decision-making level members of the data processor, and shall have the right to report the data security situation directly to the cyberspace administration and the competent and regulatory authorities. For the avoidance of

Article 条款	Comments 意见	Recommendation 建议
		doubt, the person in charge of data security can be, or be any other position that is under the supervision of, the senior management personnel of the data processor. 数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。为免疑问，数据安全负责人可以是数据处理者的高级管理人员，或者受高级管理人员监督的任何其它职位。 The person in charge of data security might also be responsible for data security and/or PI protection according to applicable laws and rules. 数据安全负责人也可以根据适用法律和规则同时负责数据安全和/或个人信息保护职责。"
Article 29 Within fifteen business days after identifying its important data, a processor of important data shall file the	As sectoral regulators are responsible for identifying the sector's important data, we recommend that regulated sectors, such as	We suggest changing Article 29 to the following: 我们建议第 29 条可以修改为：

Article 条款	Comments 意见	Recommendation 建议
following information with the cyberspace authority at the districted city level: **第二十九条** 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括： (1) basic information about the data processor, information about the data security management organ, and the name and contact information of the person in charge of data security; （一）数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等； (2) the purpose, scale, method, scope and type of data processing, and the period and location of storage, excluding the content of data; and	financial sector, file the important data with sectoral regulators. 由于行业监管机构负责识别相关行业的重要数据，我们建议受监管的行业，例如金融行业，向金融监管机构进行重要数据方面的备案。 We recommend that the Regulations align with existing sectoral supervision structure and allow financial institutions to file once with financial regulators who could coordinate with CAC further. 我们建议本条例与现行的行业监管机制保持一致，允许金融机构向金融监管机构进行一次性备案，金融监管机构可与贵办公室进行进一步协调沟通。	"**Article 29** Within fifteen business days after identifying its important data, a processor of important data shall file the following information with the primary sectoral regulator who should further coordinate with cyberspace authority at the districted city level: **第二十九条** 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向其主管行业监管机构备案，行业监管机构应进一步与设区的市级网信部门协调~~备案~~，备案内容包括： (1) basic information about the data processor, information about the data security management organ, and the name and contact information of the person in charge of data security; （一）数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等； (2) the purpose, scale, method, scope and type of data processing, and the period and

Article 条款	Comments 意见	Recommendation 建议
（二）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身； (3) other information to be filed as required by the national cyberspace authority and the competent authorities and regulatory authorities. （三）国家网信部门和主管、监管部门规定的其他备案内容。 In the event of any major change to the purpose, scope or type of, or the data security protection measures for, data processing, refiling shall be conducted. 处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。 According to the division of responsibilities among authorities, the cyberspace authority shall share the filed information with the relevant authorities.		location of storage, excluding the content of data; and （二）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身； (3) other information to be filed as required by ~~the national cyberspace authority and~~ the competent authorities and regulatory authorities. （三）~~国家网信部门和~~主管、监管部门规定的其他备案内容。 In the event of any major change to the purpose, scope or type of, or the data security protection measures for, data processing, refiling shall be conducted. 处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。 According to the division of responsibilities among authorities, the cyberspace authority

Article 条款	Comments 意见	Recommendation 建议
依据部门职责分工，网信部门与有关部门共享备案信息。		shall share the filed information with the relevant authorities. 依据部门职责分工，网信部门与有关部门共享备案信息。”
Article 31 A processor of important data shall give priority to purchasing secure and trustworthy network products and services. **第三十一条** 重要数据的处理者，应当优先采购安全可信的网络产品和服务。	We recommend that Regulations adopt technology neutral approach and allow companies the flexibility to choose technology that best suits their business and operational needs. 我们建议本条例采取技术中立的立场，允许企业灵活选择最适合其业务和经营需要的技术。	We recommend the Article be removed. 我们建议删除本条款。
Article 32 A data processor processing important data or listed abroad shall carry out, or entrust a data security service institution to carry out, an annual assessment of data security, and no later than January 31 each year submit the data security assessment report for the prior year to the cyberspace authority at the districted city level, with the content of an annual data security assessment report to include: **第三十二条** 处理重要数据或者赴境外上市的数据处理者，应当自行或者委托	We recommend that CAC recognize entrusted processing doesn't involve transfer of control and data control is still with the data processor. Therefore, entrusted processing should not be subject to same requirements laid out for data sharing and trade, and the obligations for entrusted party should be laid out in contractual terms between data processor and entrusted party. 我们建议贵办公室承认委托处理的情形不涉及数据控制权的转移，因为数	We suggest changing the last sentence to the following: 我们建议最后一款可以修改如下： “If the assessment indicates national security, economic development or public interests may be harmed, the data processor shall not share, trade, ~~entrust the processing of,~~ or provide to abroad, data.

Article 条款	Comments 意见	Recommendation 建议
数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门，年度数据安全评估报告的内容包括： (1) the review of processing of important data; （一）处理重要数据的情况； (2) the data security risks discovered and the measures to address such risks; （二）发现的数据安全风险及处置措施； (3) the data security management system, data backup, encryption, access control and other security protection measures, the implementation of the management system, and the effectiveness of the protection measures; （三）数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及	据仍由数据处理者控制。因此，委托处理不应与数据共享和交易适用同样的要求，数据受托方的义务应当在数据处理委托方与受托方之间的合同中规定。 Furthermore, for financial sector, we recommend that financial regulators should be the ones responsible for the management of "important data" of the sector and serve as point of contacts for financial institutions. Financial regulators could further coordinate with CAC. 此外，对于金融行业，我们建议金融监管机构应当负责监管本行业的"重要数据"，并作为与金融机构进行联系沟通的监管机构。金融监管机构可以与贵办公室进行进一步沟通协调。	评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、~~委托处理、~~向境外提供数据。"

Article 条款	Comments 意见	Recommendation 建议
管理制度实施情况和防护措施的有效性； (4) the implementation of the State's data security laws, administrative regulations and standards; （四）落实国家数据安全法律、行政法规和标准情况； (5) the data security incidents that have occurred and the addressing of them; （五）发生的数据安全事件及其处置情况； (6) security assessments results for sharing, trading, entrusted processing, and provision abroad of important data; （六）共享、交易、委托处理、向境外提供重要数据的安全评估情况； (7) data security-related complaints and the handling of them; and		

Article 条款	Comments 意见	Recommendation 建议
（七）数据安全相关的投诉及处理情况； (8) other information about data security specified by the national cybersecurity authority and the competent authorities and regulatory authorities. （八）国家网信部门和主管、监管部门明确的其他数据安全情况。 … If the assessment indicates national security, economic development or public interests may be harmed, the data processor shall not share, trade, entrust the processing of, or provide to abroad, data. 评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、委托处理、向境外提供数据。		
Article 33 Where a data processor shares, trades or entrusts the processing of important data, the approval from the competent authorities at the districted city	This is a new approval requirement that does not seem to have sufficient legal support under the three Laws. Our members are of the view that this approval	We would suggest CAC clarify in Article 33 that the approval requirement does not apply to data processor who does not generate such important data by itself and

Article 条款	Comments 意见	Recommendation 建议
level or above shall be obtained. If the competent authority is unclear, the approval from the cyberspace administration at the districted city level or above shall be obtained. **第三十三条** 数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。	requirement would not be relevant in the context of the financial services industry for the following reasons and we seek CAC's confirmation on such understanding: 这是一项新的同意要求，在三部数据法律中没有充分的法律支持。我们的会员认为，基于下述原因此项同意要求在金融服务业并不适用，在此我们希望获得贵办公室的确认： First of all, our members believe the financial institutions are not likely to generate "important data" directly during their ordinary course of business and to the extent that the financial institutions "process" relevant important data, another entity should have already passed the relevant test, and financial institutions that are second processors of such information should not be expected to go through the test again. 首先，我们的会员认为金融机构在其正常业务过程中不太可能直接产生"重要数据"，在金融机构"处理"相关重要	has performed necessary measures to ensure that the processing of the important data is secure and proper. 我们建议贵办公室在第 33 条中澄清：该同意要求不适用于自身不产生重要数据、且已经采取必要措施确保重要数据处理的安全性和合理性的数据处理者。

Article 条款	Comments 意见	Recommendation 建议
	数据的情况下，一般是从重要数据的提供方接收到重要数据，因此重要数据的提供方应当已经通过了相关审查，金融机构作为该等信息的次级处理者，不应被期望再次接受审查。 Secondly, the financial sector is highly regulated and financial institutions are subject to stringent outsourcing and data transferring requirements (including governance, auditing and regulatory filing requirements), and such sectoral regulations should be sufficient in ensuring financial institutions to process important data in a secure and proper manner. 其次，金融行业受到高度监管，金融机构受限于严格的外包和数据传输要求（包括内部治理、审计和监管备案要求），该等行业监管要求对于确保金融机构以安全和合理的方式处理重要数据应当足够充分。	

Article 条款	Comments 意见	Recommendation 建议
Article 34 Cloud computing services procured by the state organs and core information infrastructure operators shall be subject to security assessment organized by the Cyberspace Administration of China in concert with the relevant departments under the State Council. **第三十四条** 国家机关和关键信息基础设施运营者采购的云计算服务，应当通过国家网信部门会同国务院有关部门组织的安全评估。	We would like to clarify whether cloud computing services falls into the scope of internet services that may affect national security, which makes the CII be subject to security assessment, according to Article 35 of the CSL, i.e. a CII who procures internet products or services that may affect the national security shall be subject to the security assessment organized by the CAC. 我们希望贵办公室可以解释，本条规定的云计算服务是否属于《网络安全法》第三 35 条（即，CII 采购网络产品和服务，可能影响国家安全的，应接受贵办公室组织的安全审查）项下可能影响国家安全、将使 CII 有义务接受安全审查的网络服务？ Besides, whether a security assessment will be triggered if the cloud computing services are not purchased from third parties but are private or in-house cloud computing services?	We would respectfully request the CAC to clarify the comment in the left column and make necessary adjustment. 我们恳请贵办公室澄清左栏的问题，并作出必要的调整。

Article 条款	Comments 意见	Recommendation 建议
	此外，如果云计算服务并非从第三方购得，而是公司自有的或内部的云计算服务，是否会触发安全审查？	
Article 35 If a data processor really needs to provide data to a place outside the People's Republic of China due to its business needs, it shall meet one of the following conditions: **第三十五条** 数据处理者因业务等需要，确需向中华人民共和国境外提供数据的，应当具备下列条件之一： (1) it shall pass the security assessment for data export organized by the national cyberspace authority; （一）通过国家网信部门组织的数据出境安全评估； (2) both the data processor and the data recipient shall pass the personal information protection certification by a professional organization recognized by the national cyberspace authority;	This Article 35 as drafted relates to "data" while the matters described beneath reflect the cross-border requirements for PI. We would recommend the CAC consider the applicability of this Article and replace "data" by "PI". 目前起草的第 35 条针对的是"数据"出境要求，但其项下描述的事项反映的是对个人信息跨境传输的要求。我们建议贵办公室考虑本条的适用性，并考虑以"个人信息"取代"数据"。 Besides, we note that the exemption is consistent with the exemption from obtaining of the consent of individuals under certain circumstances set out in Article 13 of the PIPL and suggest the CAC also include additional exemptions by referring to what are considered in Article 13(ii) to 13(vii) of the PIPL.	We suggest changing Article 35 to the following to be consistent with the PIPL: 我们建议第 35 条修改如下，以与《个人信息保护法》保持一致： "**Article 35** If a PI ~~data~~ processor really needs to provide data to a place outside the People's Republic of China due to its business needs, it shall meet one of the following conditions: **第三十五条** 个人信息~~数据~~处理者因业务等需要，确需向中华人民共和国境外提供数据的，应当具备下列条件之一： (1) it shall pass the security assessment ~~for data export~~ organized by the national cyberspace authority in accordance with Article 40 of the PIPL;

Article 条款	Comments 意见	Recommendation 建议
（二）数据处理者和数据接收方均通过国家网信部门认定的专业机构进行的个人信息保护认证； (3) it shall enter into a contract with the overseas data recipient in accordance with the national cyberspace authority's requirements on standard contracts to agree on the rights and obligations of both parties; and （三）按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同，约定双方权利和义务； (4) other conditions stipulated by laws, administrative regulations or the national cyberspace authority, （四）法律、行政法规或者国家网信部门规定的其他条件。 except it is necessary for the data processor to provide to abroad the personal information of the parties to a contract for the purpose of concluding or performing the contract to which an individual is a party, or	同时，我们注意到该本条最后规定的豁免情形也是《个人信息保护法》第13条规定的在特定情况下无须取得个人同意的豁免情形，我们建议贵办公室参考《个人信息保护法》第13条第（二）项至第（七）项，在本条款中加入其它豁免事项。 Furthermore, we recommend that CAC could work in close collaboration with industry when designing standard contract terms firms could leverage for PI cross-border data transfer. 此外，我们建议贵办公室在制定标准合同条款（企业可以据此进行个人信息跨境传输）时，与相关行业保持密切合作。	（一）通过国家网信部门根据《个人信息保护法》第四十条组织的~~数据出境~~安全评估； (2) ~~both the data processor and the data recipient shall~~ pass the personal information protection certification by a professional organization recognized by the national cyberspace authority; （二）~~数据处理者和数据接收方均~~通过国家网信部门认定的专业机构进行的个人信息保护认证； (3) it shall enter into a contract with the overseas data recipient in accordance with the national cyberspace authority's requirements on standard contracts to agree on the rights and obligations of both parties; and （三）按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同，约定双方权利和义务；

Article 条款	Comments 意见	Recommendation 建议
necessary for it to provide personal information to abroad for the purpose of protecting personal life, health or property safety. 数据处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息的，或者为了保护个人生命健康和财产安全而必须向境外提供个人信息的除外。		(4) other conditions stipulated by laws, administrative regulations or the national cyberspace authority, （四）法律、行政法规或者国家网信部门规定的其他条件。 except it is necessary for the ~~data~~ PI processor to provide to abroad the personal information of the parties to a contract for the purpose of concluding or performing the contract to which an individual is a party, or necessary for it to provide personal information to abroad for the purpose of protecting personal life, health or property safety. ~~数据~~个人信息处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息的，或者为了保护个人生命健康和财产安全而必须向境外提供个人信息的除外。” We would respectfully request the CAC to consider including additional exemptions under which data processors would not be

Article 条款	Comments 意见	Recommendation 建议
		required to satisfy the requirements under Article 35 of the Regulations by referring to what is considered in Article 13(ii) to 13(vii) of the PIPL. For example, with respect to employee data, Article 13(ii) of the PIPL provides that the data processor is not required to obtain consent from employees before processing their PI if it is necessary for human resource management. We would appreciate it if the CAC could also consider such circumstance to be included in the exemption to the first paragraph of Article 35 given the necessity for MNCs to transfer employee data from their PRC operating entity to their overseas headquarters for employment management purpose, which our members believe should be considered less sensitive in the context of PRC national security and public interests. 我们恳请贵办公室可以参考《个人信息保护法》第 13 条第（二）项至第（七）项的立法意图，在第 35 条项下增加豁免数据处理者遵守本条第一款的其他情形。例如，对于员工数据，《个

Article 条款	Comments 意见	Recommendation 建议
		人信息保护法》第 13 条第（二）项规定数据处理者进行的员工个人信息处理如果是实施人力资源管理所必须，则无须事前取得员工同意。基于跨国公司为员工管理目的从其在中国的经营实体传输员工数据至其海外总部的必要性，我们期待贵办公室可以考虑将该等情形也作为对第 35 条第一款要求的例外情形，我们的会员认为，从中国国家安全和公共利益角度来看，员工数据的敏感性较低。

Article 条款	Comments 意见	Recommendation 建议
Article 36 To provide an individual's personal information to a place outside the People's Republic of China, a data processor shall inform the individual of the overseas recipient's name and contact information, the purpose and method of processing, the type of personal information, the way for the individual to exercise his/her rights to personal information against the overseas data recipient and other matters, and obtain the individual's separate consent thereto. **第三十六条** 数据处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。 If the individual's separate consent to personal information export has been obtained during the collection of personal information, and personal information will be exported in light of the agreed matters, no	We recommend CAC to reconsider the disclosure of detailed information of the receiving party as it is confidential and sensitive and could bring risks to firms' supply chain integrity. 鉴于接收方的详细信息是保密且敏感的，可能给公司的供应链完整性带来风险，我们建议贵办公室重新考虑披露接收方详细信息的要求。 Para. 2 of Article 36 (which is specifically in relation to the scenario where "separate consent" for outbound data transfer may be seen as having been obtained if relevant consent is obtained at the time of collection the PI) suggests that "separate" consent might be given to cover all the possible scenarios as long as it is separately provided at the time of information collection – we strongly suggest the CAC confirm this position in the definition of "separate consent" so as to give industry clear guidance in the implementation of this key subject in PI protection.	We would suggest CAC consider our comments in the left and make necessary adjustment. 我们建议贵办公室考虑我们左列的意见并作出必要的调整。

Article 条款	Comments 意见	Recommendation 建议
further separate consent of the individual is needed. 收集个人信息时已单独就个人信息出境取得个人同意，且按照取得同意的事项出境的，无需再次取得个人单独同意。	第 36 条第二款（即在收集个人信息时已获得对数据出境的“单独”同意可视为已获得数据出境的“单独”同意的情况）表明，只要在收集信息时另行表示同意，则被视为已经就此类所有可能的情况获得了“单独”同意。我们强烈建议贵办公室在“单独同意”的定义中确认这一立场，以便对行业就执行个人信息保护给予明确指导。	
Article 37 If a data processor provides the data collected and generated within the territory of the People's Republic of China to the recipient abroad, it shall pass the security	As for the PI, Article 37 only requires data processors who processes PI of more than one million people to apply for the security assessment, which does not expressly	We suggest that the approaches adopted in these two consultation papers shall be consistent. We would also like to recommend CAC consider our

Article 条款	Comments 意见	Recommendation 建议
assessment of the data cross-border transfer organized by the Cybersecurity Administration of China if: **第三十七条** 数据处理者向境外提供在中华人民共和国境内收集和产生的数据，属于以下情形的，应当通过国家网信部门组织的数据出境安全评估： (1) the data transferred abroad contains important data; （一）出境数据中包含重要数据； (2) the operators of critical information infrastructure and the data processors, who process the personal information of more than one million people, transfer personal information outside the territory of People's Republic of China; （二）关键信息基础设施运营者和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； (3) other circumstances as prescribed by the national cybersecurity administration.	include the scenario of outbound transfer of PI of more than 100,000 people or sensitive PI of more than 10,000 people accumulatively under Article 4(iv) of the Data Outbound Transfer Consultation Paper. 对于个人信息，第 37 条仅要求处理个人信息超过一百万人个人信息的数据处理者申请安全评估，并未明确将《数据出境征求意见稿》第 4 条第（四）项中“累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息”的情形纳入其中。	corresponding suggestions in Section 1.2 above and the separate response paper in relation to the Data Outbound Transfer Consultation Paper submitted to CAC. 我们建议两份征求意见稿的立场应保持一致。我们也建议贵办公室考虑我们在本函第 1.2 节以及在提交给贵办公室的针对《数据出境征求意见稿》的反馈意见文件中提出的相应建议。

Article 条款	Comments 意见	Recommendation 建议
（三）国家网信部门规定的其它情形。 Where laws, administrative regulations and the Cybersecurity Administration of China provide that no safety assessment is required, the provisions shall prevail. 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。		
Article 39 A data processor providing data to abroad shall perform the following obligations: **第三十九条** 数据处理者向境外提供数据应当履行以下义务： (1) it shall not provide personal information to abroad beyond the purpose, scope, method and the type and scale of data specified in the personal information protection impact assessment report submitted to the cyberspace authority; （一）不得超出报送网信部门的个人信息保护影响评估报告中明确的目的、范	Our members are of the view that imposing a statutory liability on data processors for acts of their third party contracted service providers would not be equitable and fair, particularly if such acts are due to the gross negligence or willful misconduct or other factors which are not reasonably attributable to the data processor. 我们的会员认为，让数据处理者对第三方外包服务提供商的行为承担法定责任是不公平的，尤其是如果该等行为是不可合理归咎于数据处理者的重大过失或故意不当行为或其他原因。 Article 39 (7) poses significant risks to private sectors' intellectual property and	We respectfully suggest that certain carve-outs for liability could be included. For example, liability could be excluded or limited where the liability arises out of any event that is not reasonably within the control of the data processor (such as the gross negligence or willful misconduct of the third-party service provider) provided an agreement between a data processor and the third party service provider has been properly entered into where the latter is imposed contractual obligations to ensure the security of data from the data processor. 我们诚恳地建议增加一些责任豁免情形。例如，如果是由于数据处理者不能合理控制的事件（例如第三方服务提供

Article 条款	Comments 意见	Recommendation 建议
围、方式和数据类型、规模等向境外提供个人信息； (2) it shall not provide personal information or important data to abroad beyond the purpose, scope and method of export and the type and scale of data specified during the cyberspace authority's security assessment; （二）不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供个人信息和重要数据； (3) it shall take effective measures such as signing a contract to supervise the data recipient for it to use data in accordance with the purpose, scope, and method agreed by both parties, fulfill its data security protection obligations, and guarantee data security; （三）采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式	proprietary information and should be removed entirely. 第 39 条第（七）项对私有的知识产权和专有信息构成重大风险，应当完全删除。	商的重大过失或故意不当行为），且数据处理者与第三方服务提供商已签订了适当的协议，约定第三方服务提供商须承担确保数据处理者的数据安全性的合同义务，则数据处理者的责任可以被排除或限制。 We suggest adding a qualifier in Article 39 (1) and (2) that this application is only limited to those processors who are required to submit to the CAC. 我们建议在第 39 条第（一）项和第（二）项中增加一个限定条件，即仅限于那些被要求向贵办公室报送评估报告/安全评估的数据处理者。 We strongly recommend that Article 39 (7) be removed. 我们强烈建议删除第 39 条第（七）项。 We suggest changing Article 39 (8) to the following:

Article 条款	Comments 意见	Recommendation 建议
使用数据，履行数据安全保护义务，保证数据安全； (4) it shall accept and address user complaints related to data export; （四）接受和处理数据出境所涉及的用户投诉； (5) if the data export causes any damage to an individual's or organization's legal rights or interests or public interests, the data processor shall be liable therefor in accordance with the law; （五）数据出境对个人、组织合法权益或者公共利益造成损害的，数据处理者应当依法承担责任； (6) it shall keep the relevant log records and data export approval records for no less than three years; （六）存留相关日志记录和数据出境审批记录三年以上；		我们建议将第 39 条第八项修改为： "(8) if the national cyberspace authority determines no export should be permitted according to laws and regulations, the data processor shall stop its data export, and take effective remedial measures for the security of the data exported; and…" （八）国家网信部门依法认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救…"

Article 条款	Comments 意见	Recommendation 建议
(7) when the national cyberspace authority and the relevant departments of the State Council verify the type and scope of personal information or important data provided to abroad, the data processor shall present the same in an explicit and readable form; （七）国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示； (8) if the national cyberspace authority determines no export should be permitted, the data processor shall stop its data export, and take effective remedial measures for the security of the data exported; and （八）国家网信部门认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救； (9) if an individual's personal information really needs to be retransferred after being exported, it shall agree with the individual on		

Article 条款	Comments 意见	Recommendation 建议
the conditions for retransfer in advance, and specify the security protection obligations to be performed by the data recipient. （九）个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。 Without approval by the competent authorities of the People's Republic of China, no individual or organization within the territory the People's Republic of China shall provide any foreign judicial or law enforcement agency with any data stored in the People's Republic of China. 非经中华人民共和国主管机关批准，境内的个人、组织不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。		
Article 40 Data processors who provide personal information and important data outside the territory of the People's Republic of China shall prepare a cross-border data transfer security report by January 31 of each year and report to the municipal cybersecurity	Article 40 is in addition to the data security assessment under Article 32, prefecture-level city approval under Article 33 and the CAC security assessment under the PIPL and/or the Data Outbound Transfer Consultation Paper. We would respectfully	We suggest revising the first paragraph of Article 40 as follow: 我们建议对第 40 条第（一）款作如下修改：

Article 条款	Comments 意见	Recommendation 建议
administration about the following cross-border data transfer situation of the previous year: **第四十条** 向境外提供个人信息和重要数据的数据处理者，应当在每年 1 月 31 日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况： (1) the name and contact details of all data recipients; （一）全部数据接收方名称、联系方式； (2) the type, quantity and purpose of the cross-border transferred data; （二）出境数据的类型、数量及目的； (3) where, during which the data are stored outside the territory of the People's Republic of China, the duration of storage, the scope of use and the manner in which it is used;	suggest that the CAC consider to limit the scope of Article 40 (e.g. to apply only to data processors who are required to pass the CAC security assessment for outbound transfer) and/or to rationalized these requirements into one integrated regime. 第 40 条是对第 32 条项下的数据安全评估、第 33 条项下的设区的市级主管部门的同意以及《个人信息保护法》和/或《数据出境征求意见稿》项下的网信部门组织的安全评估的补充。我们谨建议，贵办公室可以考虑限制第 40 条的适用范围（例如仅适用于需要通过贵办公室安全评估才能进行数据出境的数据处理者）和/或将这些要求整合为一个完整的制度。 We recommend a streamlined regulatory framework where financial regulators are responsible for the sector-wide data security and interacting with financial institutions. Financial regulators should further	"**Article 40** Data processors who provide personal information and important data outside the territory of the People's Republic of China and be subject to the CAC security assessment requirements shall prepare a cross-border data transfer security report by January 31 of each year and report to the primary sectoral regulator who should coordinate with the municipal cybersecurity administration about the following cross-border data transfer situation of the previous year:… **第四十条** 向境外提供个人信息和重要数据并需要通过网信部门组织的安全评估的数据处理者，应当在每年 1 月 31 日前编制数据出境安全报告，并向行业主管部门报告上一年度以下数据出境情况，行业主管部门应当与设区的市级网信部门协调: …" In addition to the above, we suggest that the requirements listed in Article 40 shall be rationalized with existing regimes to the extent possible.

Article 条款	Comments 意见	Recommendation 建议
（三）数据在境外的存放地点、存储期限、使用范围和方式； (4) the complaints and handling of user complaints relating to the cross-border data transfer; （四）涉及向境外提供数据的用户投诉及处理情况； (5) the data security incidents occurred and their disposition; （五）发生的数据安全事件及其处置情况； (6) the situation of re-transfer after the data transferred outside the territory of the People's Republic of China; （六）数据出境后再转移的情况； (7) other matters that the Cybersecurity Administration of China required to be reported for the cross-border data transfer. （七）国家网信部门明确向境外提供数据需要报告的其他事项。	coordinate with the CAC on data security matters. 我们建议建立一个简化的监管框架，由金融监管部门负责全行业的数据安全并与金融机构沟通。金融监管部门应就数据安全事宜与贵办公室进一步协调。	此外，我们建议第 40 条中的要求应尽可能与现有的规则制度相协调。

Article 条款	Comments 意见	Recommendation 建议
Article 41 The State is to establish a cross-border data transfer security gateway to block the spread of information that originates outside the People's Republic of China and is prohibited by a law or administrative regulation from being released or transmitted. **第四十一条** 国家建立数据跨境安全网关，对来源于中华人民共和国境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。 No individual or organization shall provide programs, tools, or lines to be used for penetrating or bypassing the cross-border data transfer security gateway, or provide Internet access, server hosting, technical support, dissemination or promotion, payment clearing, application downloading or other services for penetrating or bypassing the cross-border data transfer security gateway. 任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线	Existing rules and regulations on VPNs and existing gateways and other technical measures already place strict controls on VPN, content and others. Suggest to delete as those proposals duplicate existing efforts with no additional value-add. 有关 VPN 的现有法规规则以及现有的网关和其他技术措施已经对 VPN、内容和其他方面进行了严格控制。因此我们建议删除第 41 条的规定，其仅是对现有规则的重复，没有额外的价值。 We seek clarification of the meaning of the key terms in the Article, including "penetrating", "traffic," "domestic network" and "routed to abroad". 我们希望贵办公室可以澄清该条款中某些重要术语的含义，包括"穿透"、"流量"、"境内网络"和"路由至境外"。	We suggest removing this Article completely. 我们建议完全删除本条。 If the draft Regulations is to retain requirement of traffic routing overseas, we recommend significantly expanding the level of detail in Article 41. At a minimum, member companies require assurances that subsidiaries of foreign companies, or foreign companies themselves operating in China, use legitimate corporate VPNs, provided that China's telecom providers are not viewed as domestic users and are carved out. It's critical that foreign companies and its China subsidiaries are permitted to talk freely, which is fundamental to the operation of the Internet and multinational companies today. 如果本条例拟保留流量不得被路由至境外的要求，我们建议尽量细化第四十一条的规定。至少，我们的会员恳请确认境外公司的子公司或境外公司本身在中国经营时可以使用合法的企业 VPN，

Article 条款	Comments 意见	Recommendation 建议
路等，不得为穿透、绕过数据跨境安全网关提供互联网接入、服务器托管、技术支持、传播推广、支付结算、应用下载等服务。 The traffic of domestic users accessing domestic networks may not be routed to abroad. 境内用户访问境内网络的，其流量不得被路由至境外。		如果中国的电信服务提供商将不会被视为境内用户而得到豁免。允许外国公司及其在中国的子公司能够自由地沟通交流是至关重要的，且是当今的互联网和跨国企业运营的基础。
Article 42 A data processor engaged in cross-border data transfer activities shall establish and perfect the relevant technical and management measures in accordance with the State's requirements for cross cross-border data transfer security supervision. **第四十二条** 数据处理者从事跨境数据活动应当按照国家数据跨境安全监管要求，建立健全相关技术和管理措施。	We recommend that Article 42 to studiously follow the scope and regulatory framework established in the DSL, the PIPL and the CSL and not expand the scope to cover all firms and activities involving non PI and non-important data. 我们建议第 42 条严格遵循《数据安全法》、《个人信息保护法》和《网络安全法》的适用范围和监管框架，不要将范围扩大到处理非个人信息和非重要数据的所有公司及其活动。	We suggest removing the Article. If the Article is to be retained, we suggest changing Article 42 to the following to be consistent with the PIPL, the CSL and the DSL: 我们建议删除该条款。如果保留该条款，为与《个人信息保护法》、《网络安全法》和《数据安全法》保持一致，我们建议将第 42 条修改如下： "**Article 42** A PI ~~data~~ processor or an important data processor engaged in cross-border data transfer activities shall establish and perfect the relevant technical and

Article 条款	Comments 意见	Recommendation 建议
		management measures in accordance with the laws and regulations ~~State's requirements for cross-cross-border data transfer security supervision~~. 第四十二条 个人信息~~数据~~处理者或重要数据处理者从事跨境数据活动应当按照法律法规的~~国家数据跨境安全监管~~要求，建立健全相关技术和管理措施。”
Article 55 The national cyberspace authority is responsible for the overall planning and coordination of data security and related supervision and management. **第五十五条** 国家网信部门负责统筹协调数据安全和相关监督管理工作。 The public security, national security and other relevant authorities are responsible for data security supervision within the scope of their respective duties. 公安机关、国家安全机关等在各自职责范围内承担数据安全监管职责。 The competent authorities in charge of industry, telecommunications,	For financial sector, we recommend that financial regulators should be the ones responsible for the management of “important data” of the sector and serve as point of contacts for financial institutions when it comes to reporting and other requirements for “important data”. Financial regulators could further coordinate with CAC. 对于金融业，我们认为应由金融监管机构负责该行业“重要数据”的监管，并在涉及“重要数据”的报告和其他要求时作为对接金融机构的主体。金融监管机构可以与贵办公室进一步沟通协调。	We suggest CAC consider our recommendation and make such principle clearer in Article 55. 我们希望贵办公室考虑我们的建议，并在第 55 条中更清晰地体现这一原则。

Article 条款	Comments 意见	Recommendation 建议
transportation, finance, natural resources, hygiene and health, education, and science and technology are responsible for data security supervision in their respective industries and fields. 工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。 The competent authorities shall specify the data security protection organs and personnel in their respective industries and fields, develop and organize the implementation of data security plans and emergency data security incident response plans for their respective industries and fields. 主管部门应当明确本行业、本领域数据安全保护工作机构和人员，编制并组织实施本行业、本领域的数据安全规划和数据安全事件应急预案。 The competent authorities shall regularly organize and carry out data security risk assessments in their respective industries and		

Article 条款	Comments 意见	Recommendation 建议
fields, supervise and inspect data processors' fulfillment of their data security protection obligations, guide and urge data processors to rectify existing risks and hidden dangers in a timely manner. 主管部门应当定期组织开展本行业、本领域的数据安全风险评估，对数据处理者履行数据安全保护义务情况进行监督检查，指导督促数据处理者及时对存在的风险隐患进行整改。		
Article 56 The State is to establish and perfect an emergency data security response mechanism, improve the emergency cyber security incident response plan and the cyber security information sharing platform, incorporate data security incidents into the national emergency cyber security incident response mechanism, and strengthen the sharing of data security information, the monitoring and early warning of data security risks and threats, and the emergency addressing of data security incidents. **第五十六条** 国家建立健全数据安全应急处置机制，完善网络安全事件应急预	We recommend a streamlined emergency response mechanism that places sectoral regulators as the coordinating body with their respective sectors, and establish a mechanism for sectoral regulators to further coordinate with the national body. This could reduce duplication of work and allow for better sectoral holistic view and oversight. 我们建议建立一个精简高效的应急处置机制，行业监管机构作为各个行业的协调机构，并为行业监管机构与国家机构的进一步协调建立相关机制。	

Article 条款	Comments 意见	Recommendation 建议
案和网络安全信息共享平台，将数据安全事件纳入国家网络安全事件应急响应机制，加强数据安全信息共享、数据安全风险和威胁监测预警以及数据安全事件应急处置工作。	这样可以减少重复工作，并促进对行业的整体观察和监督。	
Article 57 The relevant competent authorities and regulatory authorities may supervise and inspect data security by taking the following measures: **第五十七条** 有关主管、监管部门可以采取以下措施对数据安全进行监督检查： (1) requiring data processors and relevant personnel to explain the matters under supervision or inspection; （一）要求数据处理者相关人员就监督检查事项作出说明； (2) accessing or retrieving data security-related documents and records;	We strongly advocate against testing and connecting testing tools to companies' network. Tests pose real risks to firms operating globally due to the potentially disruptive nature of such testing. Testing systems and application without operational context could create significant disruption to firms' operations. In the inter-connected financial sector, such testing could lead to financial stability events that disrupt the financial system globally. 我们对检测，以及检测工具与企业的网络的连接表示强烈反对，因为检测可能存在的危害性，会给跨国企业带来实际风险。非运营环境下的检测系统和应用程序可能会对企业的运营造成重大干扰。在关联紧密的金融行	We suggest changing Article 57 to the following: 我们建议将第 57 条修改如下： "**Article 57** The relevant competent authorities and regulatory authorities may supervise and inspect data security in accordance with laws and regulations by taking the following measures: **第五十七条** 有关主管、监管部门可以根据法律法规采取以下措施对数据安全进行监督检查： (1) requiring data processors and relevant personnel to explain the matters under supervision or inspection;

Article 条款	Comments 意见	Recommendation 建议
（二）查阅、调取与数据安全有关的文档、记录； (3) using testing tools or entrusting professional institutions to conduct technical testing on the implementation of data security measures in accordance with the prescribed procedures; （三）按照规定程序，利用检测工具或者委托专业机构对数据安全措施运行情况进行技术检测； (4) verifying the type and scope of the exported data; and （四）核验数据出境类型、范围等； (5) other necessary methods stipulated by laws, administrative regulations and rules. （五）法律、行政法规、规章规定的其他必要方式。 The relevant competent authorities and regulatory authorities shall conduct data security supervision and inspection	业，检测可能影响金融稳定，干扰全球金融体系的正常秩序。 The testing result is highly sensitive and critical to firms and should be kept close hold by firms, not shared with any 3rd party. 检测结果对于企业来说是高度敏感和关键的，应该由企业掌握，不应与任何第三方共享。 We recommend that CAC recognize the importance of protection of proprietary information and trade secrets and recommend deletion of "permitting the access to security related data and providing necessary technical supports". 我们希望贵办公室认识到保护专有信息和商业秘密的重要性，并删除"开放安全相关数据访问、提供必要技术支持"这一要求。 We would like to work with CAC and together come up with reasonable measures in accordance with laws and regulations that	（一）要求数据处理者相关人员就监督检查事项作出说明； (2) accessing or retrieving data security-related documents and records; （二）查阅、调取与数据安全有关的文档、记录； ~~(3) using testing tools or entrusting professional institutions to conduct technical testing on the implementation of data security measures in accordance with the prescribed procedures;~~ ~~（三）按照规定程序，利用检测工具或者委托专业机构对数据安全措施运行情况进行技术检测；~~ (~~4~~3) verifying the type and scope of the exported data; and （~~四~~三）核验数据出境类型、范围等； (~~5~~4) other necessary methods stipulated by laws, administrative regulations and rules.

Article 条款	Comments 意见	Recommendation 建议
objectively and fairly, and shall not charge fees from the inspected units. The information obtained during the data security supervision and inspection may only be used for the maintenance of data security, and shall not be used for other purposes. 有关主管、监管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用。在数据安全监督检查中获取的信息只能用于维护数据安全的需要，不得用于其他用途。 Data processors shall cooperate with relevant competent authorities and regulatory authorities in their data security supervision and inspection, including explaining organizational operations, technical systems, algorithm principles and data processing procedures, permitting the access to security-related data, and providing necessary technical supports, etc. 数据处理者应当对有关主管、监管部门的数据安全监督检查予以配合，包括对组织运作、技术系统、算法原理、数据	could meet policy goals without imposing such risks to businesses. 我们希望与贵办公室合作，根据法律法规协助制定既能达到政策目标，又不会给企业业务带来风险的合理措施。	（~~五~~四）法律、行政法规、规章规定的其他必要方式。 The relevant competent authorities and regulatory authorities shall conduct data security supervision and inspection objectively and fairly, and shall not charge fees from the inspected units. The information obtained during the data security supervision and inspection may only be used for the maintenance of data security, and shall not be used for other purposes. 有关主管、监管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用。在数据安全监督检查中获取的信息只能用于维护数据安全的需要，不得用于其他用途。 Data processors shall cooperate with relevant competent authorities and regulatory authorities in their data security supervision and inspection, including explaining organizational operations, technical systems, algorithm principles and

Article 条款	Comments 意见	Recommendation 建议
处理程序等进行解释说明，开放安全相关数据访问、提供必要技术支持等。		data processing procedures~~, permitting the access to security-related data, and providing necessary technical supports, etc~~. 数据处理者应当对有关主管、监管部门的数据安全监督检查予以配合，包括对组织运作、技术系统、算法原理、数据处理程序等进行解释说明~~，开放安全相关数据访问、提供必要技术支持等~~。”
Article 58 The State is to establish a data security audit system. Data processors shall entrust professional data security audit institutions to regularly audit the compliance of their personal information processing with laws and administrative regulations. **第五十八条** 国家建立数据安全审计制度。数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。 The competent authorities and regulatory authorities shall organize and carry out audits of important data processing activities, which shall be focused on the data processors'	We highly recommend that the audit requirement only applies to the data processors meeting criteria laid down in Article 37 of the Regulations, namely “CIIOs” “PI processors with 1 million PI” and “firms with important data”. Mandating audit for all data processors, especially SMEs, would incur unnecessary costs and burdens without properly focusing on risks. 我们强烈建议审计要求仅适用于本条例第 37 条项下的数据处理者，即“CII 运营者”、“处理一百万人以上个人信息的数据处理者”和“重要数据处理者”。要求所有数据处理者，特别是中小企业进行审计，将给这些企造成不	We suggest changing Article 58 to the following: 我们建议将第 58 条修改如下： **“Article 58** The State is to establish a data security audit system. ~~Data~~PI processors of over 1 million PI and “important data” processors can leverage international standards and certification, and can ~~shall~~ entrust professional data security audit institutions to regularly audit the compliance of their personal information processing with laws and administrative regulations. **第五十八条** 国家建立数据安全审计制度。处理一百万人以上个人信息的个人

Article 条款	Comments 意见	Recommendation 建议
fulfillment of obligations stipulated in the laws and administrative regulations. 主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。	必要的成本和负担，从而分散其监测相关数据风险的注意力。 In addition, we recommend that CAC recognize international standards and certification. 此外，我们建议贵办公室能够承认国际标准和认证。	信息~~数据~~处理者可以按照国际标准和认证要求，并可以~~应当~~委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。 The competent authorities and regulatory authorities shall organize and carry out audits of important data processing activities, which shall be focused on the data processors' fulfillment of obligations stipulated in the laws and administrative regulations. 主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。"
Article 59 The State supports the relevant industry organizations to formulate codes of conduct for data security in accordance with their articles of association, strengthen industry self-discipline, guide their members to enhance data security protection, improve their level of data security	Any self-discipline convention and industry organization should be market-driven and developed and organized on a voluntary-basis. The article should be removed to leave the market be the driving force for such voluntary association.	We recommend this Article be removed. 我们建议删除本条。

Article 条款	Comments 意见	Recommendation 建议
protection, and promote the healthy development of their industries. **第五十九条** 国家支持相关行业组织按照章程，制定数据安全行为规范，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。 The State supports the establishment of an industry organization for personal information protection to carry out the following activities: 国家支持成立个人信息保护行业组织，开展以下活动： (1) accepting complaints and whistleblowing reports regarding personal information protection, and conduct investigations and mediation; （一）接受个人信息保护投诉举报并进行调查、调解； (2) providing information and consulting services to individuals, and supporting	任何自律公约和行业组织都应该是市场主导，且在自愿的基础上发展和成立的。我们建议删除本条，留给市场自身去决定该等自律组织的成立与否。	

Article 条款	Comments 意见	Recommendation 建议
individuals to file lawsuits against the activities that damage personal information rights and interests in accordance with the law; （二）向个人提供信息和咨询服务，支持个人依法对损害个人信息权益的行为提起诉讼； (3) exposing activities that damage personal information rights and interests, and conducting public supervision over personal information protection; （三）曝光损害个人信息权益的行为，对个人信息保护开展社会监督； (4) reporting information about personal information protection, and providing advice and suggestions to the relevant authorities; and （四）向有关部门反映个人信息保护情况、提供咨询、建议； (5) filing a lawsuit to the people's court in accordance with the law with respect to the		

Article 条款	Comments 意见	Recommendation 建议
acts of illegally processing personal information or infringing on the rights and interests of many individuals. （五）违法处理个人信息、侵害众多个人的权益的行为，依法向人民法院提起诉讼。		
Article 73 The meanings of the following terms used herein are as follows: **第七十三条** 本条例下列用语的含义： (1) "Network data" (herein referred to as "data") means any electronic record of information. （一）网络数据（简称数据）是指任何以电子方式对信息的记录。 (2) "Data processing activities" means the collection, storage, use, processing, transmission, provision, publication and deletion of data. （二）数据处理活动是指数据收集、存储、使用、加工、传输、提供、公开、删除等活动。	The inability to gain a clear understanding of what constitutes "important data" has created tremendous uncertainty for companies. We recommend that sectorial regulator work in close collaboration with companies in developing important data catalogue and narrowly scope important data. "重要数据"含义的不明确给企业经营带来了巨大的不确定性。我们建议行业监管机构与企业可以密切合作，制定重要数据清单，并缩小重要数据的范围。 The definition given for "core data" is very similar, if not the same, with "important data". We seek clarification on the differences between the two categories.	We suggest that greater clarity could be provided to organizations across different industries and the public regarding the timing, scope and attributes of sectoral regulators' forthcoming important data catalogues, as the inclusion of certain types of data in these documents will have significant implications for businesses and their partners. Additionally, we believe the definition for "important data" should reference the draft CAC Data Security Management Measures in 2019 to exclude enterprise production management and internal business operations data. 我们希望，贵办公室可以向不同行业及社会上组织就行业主管机构即将颁布的重要数据目录的时点、范围以及特征提供更多澄清，因为在该等目录中加入特

Article 条款	Comments 意见	Recommendation 建议
(3) "Important data" means any data whose tampering, corruption, leakage or illegal obtainment or use may endanger national security or public interests, including: （三）重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。包括以下数据： 1. unpublished government data, work secrets, intelligence data, and law enforcement or judicial data; 未公开的政务数据、工作秘密、情报数据和执法司法数据； 2. data that are subject to export control, data related to the core technologies, design plans, or production processes of items subject to export control, and data related to scientific and technological achievements in the fields of cryptography, biology, electronic information, or artificial intelligence that have a direct impact on national security or economic competitiveness;	目前"核心数据"与"重要数据"的定义非常相似，我们希望就者两类数据之间的区别得到进一步的澄清。	定数据类型将会对业务以及合作方产生重大影响。此外，我们相信"重要数据"的定义将会参考贵办公室在 2019 年颁布的《数据安全管理办法（征求意见稿）》，即将企业生产经营和内部管理信息排除在重要数据之外。 We suggest providing clearer differentiation of the definition of "important data" and "core data". 我们建议贵办公室对"重要数据"和"核心数据"的定义进行更明确的区分。

Article 条款	Comments 意见	Recommendation 建议
出口管制数据，出口管制物项涉及的核心技术、设计方案、生产工艺等相关的数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争实力有直接影响的科学技术成果数据； 3. data related to operation of the national economy, business data in key industries, and statistical data that are subject to protection or control of transmission as expressly provided in a national law, an administrative regulation or a departmental rule; 国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等； 4. data related to safe production and operation and data related to key system components or equipment supply chains in key industries or fields		

Article 条款	Comments 意见	Recommendation 建议
including industry, telecommunications, energy, transportation, water resources, finance, national defense technology, customs and taxation; 工业、电信、能源、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据； 5. fundamental national data related to health and demography, natural resources and the environment, including genetics, geography, mining or meteorology that has reached the scale or precision specified by the relevant authorities of the State; 达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等人口与健康、自然资源与环境国家基础数据； 6. data related to the construction, operation or security of national		

Article 条款	Comments 意见	Recommendation 建议
infrastructure or critical information infrastructure, and data related to the geographic location or security of sensitive key areas, including national defense facilities, military management zones, and scientific research or production units for national defense; and 国家基础设施、关键信息基础设施建设运行及其安全数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据； 7. other data that may have an impact on the security of national politics, homeland, the military, the economy, culture, society, technology, ecology, resources, nuclear facilities, overseas interests, biology, space, polar regions or deep seas. 其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生		

Article 条款	Comments 意见	Recommendation 建议
物、太空、极地、深海等安全的数据。 (4) "Core data" means any data related to national security, the lifelines of the national economy, important social welfare, or major public interests…. （四）核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据….		