28 May 2021

2021 年 5 月 28 日

National People's Congress of the People's Republic of China Legislative Affairs Commission

No.1 Qianmen West Street, Xicheng District

Beijing, China

100805

全国人大常委会法制工作委员会

西城区前门西大街 1 号

北京，中国

邮编：100805

To the Commission
致：法工委

Consultation Draft of the Second Review of the Data Security Law

《数据安全法》（草案二次审议稿）征求意见

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] ("**we**", "**our**" or "**us**") are pleased to submit to the Legislative Affairs Commission of the Standing Committee of the 13th National People's Congress ("**Commission**") our comments and suggestions on the Consultation Draft of the Second Review of the Data Security Law ("**Second Review DSL**") of the People's Republic of China ("**PRC**") published on the National People's Congress website[2].

亚洲证券业与金融市场协会（"**ASIFMA**"）[1]（统称"**协会**"或"**我们**"）谨代表协会全体成员表示，很荣幸有机会就中国人大网发布的《中华人民共和国数据安全法》（草案二次审议稿）征求意见（"**数据安全法（草案二次审议稿）**"）向第 13 届全国人大常委会法制工作委员会（"**法工委**"）提出意见和建议[2]。

As we did for our submission on the Consultation Draft of the First Review of the Data Security Law of the PRC ("**First Review DSL**"), we have consulted our members and received responses. This letter sets out our views on the Second Review DSL, the practical difficulties financial institutions may face and our recommendations and our requests for clarification of certain provisions of the Second Review DSL.

与《数据安全法》（草案一次审议稿）征求意见（"**数据安全法（草案一次审议稿）**"）相同，协会已征求协会会员意见并得到积极回应。本函件载列我们关于数据安全法（草案二次审议稿）的意见、金融机构可能面临的实际困难、我们的建议以及我们希望数据安全法（草案二次审议稿）的若干条文能够更为明晰的请求。

---

[1] ASIFMA is an independent, regional trade association with over 140 member firms comprising a diverse range of leading financial and professional institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

ASIFMA 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 140 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。我们在金融行业拥有共同的利益，即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。ASIFMA 认为拥有一个稳定、创新、竞争和高效的亚洲资本市场对于支持亚洲地区的经济增长是十分关键的。我们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。我们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。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。

[2] Available at: http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80818178f9100801791b3c96374eef.
可于以下网址查阅：http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80818178f9100801791b3c96374eef。

In summary, we support the need for jurisdictions to establish reasonable and proportionate mechanisms to safeguard data. Data is pivotal to the business of our members, and concomitant controls are essential to the integrity of financial markets and business confidence more broadly.

总括而言，我们明白各司法管辖区建立合理及适当的机制保护数据安全的需要。数据不仅是本协会成员进行业务经营的关键，更广泛而言，数据相关管制措施对健全金融市场及稳定经营者信心至关重要。

At the same time, the Second Review DSL – as was the case for the First Review DSL – casts a broad net and, in certain instances is difficult to interpret in practice and can be open to significant interpretation. Its interaction with existing legal and regulatory requirements and expectations – in particular the Cybersecurity Law ("**CSL**") and the future Personal Information Protection Law ("**PIPL**") – is also unclear.

同时，数据安全法（草案二次审议稿）（与数据安全法（草案一次审议稿）相同）涵盖范围广泛，在部分情况下难以作出具体解释或可以有各种不同的解读。数据安全法与现有法律法规（尤其是《网络安全法》（"**网络安全法**"）的要求和期望，以及将来的《个人信息保护法》（"**个人信息保护法**"）之间的关系和相互影响尚不明确。

The **Appendix** sets out our detailed comments.

我们的详细意见载于**附件**。

Next steps

下一步行动

We would be pleased to engage in further discussions with the Commission in relation to our comments and provide further industry input where necessary. If you have any questions, please contact Matthew Chan, ASIFMA Head of Policy and Regulatory Affairs, at mchan@asifma.org or +852 2531 6560.

我们很乐意与法工委进一步探讨我们的意见，并在有需要时进一步提供业界意见。如果您有任何疑问，请联系 ASIFMA 政策和法规事务总监 Matthew Chan（电邮：mchan@asifma.org，电话：+852 2531 6560）。

In the meantime, to facilitate dialogue, we will also share a copy of our submission with the People's Bank of China and China Securities and Regulatory Commission, given the potential overlapping areas of regulation.

同时，为方便就监管可能重叠的领域展开交流，本函件会抄送中国人民银行和中国证券监督管理委员会。

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

本函件在昭胜年利达（自贸区）联营办公室的协助下，根据 ASIFMA 会员的广泛反馈意见撰写。

Yours faithfully,

顺颂商祺

Matthew Chan
Head of Policy and Regulatory Affairs, Asia Pacific
Asia Securities Industry & Financial Markets Association
(ASIFMA)

Appendix – Detailed comments
附件 – 具体意见

Introduction

绪言

This Appendix is structured as follows:

Part A **甲部**	General and overarching comments 一般和整体意见
Part B **乙部**	Specific comments on each article 有关各条款的具体意见

Unless otherwise specified, terms used in this appendix have the meaning and construction given to them in the letter or the Second Review DSL; any reference to the "**Second Review DSL**" is a reference to the draft of the Data Security Law ("**DSL**") published on the National People's Congress website as at the date of this submission; and any reference to an Article is to an Article of the Second Review DSL.

除非另有说明，本附件所用词汇具有本函件或数据安全法赋予其的涵义，并应根据本函件或数据安全法（草案二次审议稿）解释；"**数据安全法（草案二次审议稿）**"指截至本函件日期在中国人大网所登载的《数据安全法》（"**数据安全法**"）草案；凡提及某一条款之处均是指数据安全法（草案二次审议稿）中的条款。

Part A Overarching comments

甲部 整体意见

1. Principle-based obligations

原则性义务

We understand that the DSL sets out general principles and anticipates relevant authorities to formulate more specific rules.

我们知悉，数据安全法载有一般性原则，并预期相关主管机构会制定进一步的细则。

That said, certain provisions (primarily Chapter IV of the DSL) directly impose obligations on all companies, including financial institutions. We submit that these provisions are not sufficiently specific for financial institutions to understand the expectations of the DSL and the relevant authorities, and they cannot effectively assess their legal and compliance obligations against their existing business practice.

即便如此，部分条文（主要是数据安全法第四章）还是会直接对包括金融机构在内的所有公司施加义务。我们认为，该等条文不够具体，不足以让金融机构了解数据

安全法和相关主管机构想达到的预期效果，因此金融机构无法有效评估其现有业务活动的法律和合规义务。

This is particularly the case for foreign financial institutions with a view to developing their businesses in the PRC. The broadly worded obligations may give rise to uncertainties as to their legal and compliance obligations and risks, how breaches of the obligations may be enforced, and how their business operations will be affected. This may discourage the entry and/or continued operation of many foreign financial institutions, particularly where there are cross-border aspects to their business or where they seek to leverage the benefits of global expertise and centralised infrastructure, risk or control functions. It is also likely to cause confusion for those using the services of onshore data partners. This is supported by the 2021 China Business Climate Survey Report released by AmCham China,[3] which noted that inconsistent regulatory interpretation and unclear laws and enforcement is a top challenge for the services sector.

如果境外金融机构有意在中国发展业务，情况更是如此。描述宽泛的义务会造成多方面的不确定性，包括法律及合规义务和风险、在违反义务的情况下会被如何执法以及其业务经营会受到怎样的影响。这可能会打击众多境外金融机构进入中国及/或继续在中国经营的积极性，尤其是涉及跨境业务或寻求利用其国际专业知识优势和基建、风险或监控职能集中管理优势的机构。此外，就使用中国本地数据合作者提供的服务的境外机构而言，义务的描述过于宽泛亦可能造成混淆。中国美国商会发布的 2021 年中国商务环境调查报告提到 [3]，法律法规解释执行不一致/不明确是服务行业面临的最大挑战之一，也印证了这一情况。

We recommend the Commission consider:

我们建议法工委考虑下列各项：

(a) having a lead, or coordinating, regulator (e.g. the People's Bank of China ("**PBOC**")) in implementing the DSL for the financial services sector, including for the purposes of formulating further rules or regulations in respect of the application of the DSL to the financial services sector, and how they are enforced;

由一个牵头或协调监管机构（如中国人民银行（"**央行**"））在金融服务行业全面施行数据安全法，包括就数据安全法在金融服务行业的应用以及如何执法制定进一步规则或法规；

(b) expressly acknowledging the relevant lead regulator (e.g. PBOC)'s detailed guidance and practical examples on how financial institutions can discharge their obligations, with:

[3] Available at: https://portal.amchamchina.org/#/custom/FileDownLoadList. See page 58 of the report.
查阅报告：https://www2.deloitte.com/cn/zh/pages/about-deloitte/articles/deloitte-amcham-2019-china-business-climate-survey-report.html。详见报告第 40 页。

明确承认有关牵头监管机构（如央行）就金融机构履行义务的方式方法所制定的详细的指引和应用实例，并且

(i) a transparent and inclusive process that engages with market participants (directly or through industry associations) in the drafting process, to ensure that these guidelines are ultimately practicable and workable;

采用透明及具包容性的程序，在起草阶段允许市场从业者（直接或通过行业协会）参与，以确保该等指引目前是最终切实可行且行之有效的；及

(ii) a collaborative approach between authorities to ensure the core aspects of the DSL are consistently implemented by each sector, and reduce the likelihood of regulatory arbitrage;

通过各主管机构合作，确保数据安全法的核心内容在各个行业一致实施，减少监管套利的可能性；

(c) that rules, regulations or guidance applicable on a sectoral basis ("**sectoral rules**") should prevail over those:

按行业应用的规则、法规或指引（"**行业规则**"）的适用性应优于：

(i) set out in the framework of the DSL. Specifically, instead of including references in an article or provision as to where administrative regulations would prevail, there should be a clear statement that sectoral implementing regulations are supplementary and prevail over the overarching laws such as the DSL; and

数据安全法框架内的规则。具体而言，不是在某一条文或规定中提及行政规章将在哪些领域优先适用，而应明确说明按行业实施的规定具有补充性，其适用性优于数据安全法等原则性法律；及

(ii) applicable based on the location of the data processing (that is, if a national financial regulator specifies certain sectoral rules, then these sectoral rules should prevail over any general rules specified by a local authority in the place where the data processing occurs);

按数据处理所在地应用的规则（也就是说，如果国家金融监管机构订明若干行业规则，则该等行业规则的适用性应优于开展数据处理发生地的地方主管机构制定的任何一般规则）；

(d) any new sectoral rules for the financial sector either replace or expressly supplement existing rules, to avoid overlap; and

任何金融行业新制定的行业规则应替代或是明确补充现行规则以避免范围重叠；及

(e) that sectoral rules take effect at the same time as the DSL, with an adequate implementation period. We suggest this period should be at least 24 months. If, for any reason, the sectoral rules cannot take effect at the same time as the DSL, we suggest an implementation period of 24 months after the sectoral rules are finalised to enable financial institutions to fully understand the implications and formulate and implement the necessary compliance measures.

行业规则与数据安全法同时生效，并给予适当的执行期间（我们建议最少为24个月）。如果行业规则因任何原因未能与数据安全法同时生效，我们建议在落实行业规则后给予 24 个月的执行期，让金融机构能够充分了解有关影响，制定和实施必需的合规措施。

2. Overlap with existing laws and regulations

与现有法律法规重叠

The wide scope of application of the DSL causes overlap with existing laws, regulations and guidelines. For example, the CSL covers "*network data*" which refers to "*all kinds of electronic data collected, stored, transmitted, processed and produced through the networks*". Where there is any inconsistency in the overlapping parts among the DSL, the existing CSL and their respective subsidiary legislation and guidance, it is unclear whether the principle of "a special law prevails over a general law" or the principle of "a new law prevails over an old law" apply. Similarly, the Civil Code of the PRC, which took effect on 1 January 2021, contains provisions relating to personal data protection and privacy.

数据安全法的应用范围广泛，导致与现行法律、法规和指引的应用范围重叠。例如，网络安全法涵盖"*网络数据*"，网络数据是指"*通过网络收集、存储、传输、处理和产生的各种电子数据*"。如果数据安全法及其附属法律及指引和现行的网络安全法及其附属法律及指引之间有任何不一致或重叠部分，则如何应用"*特别法优于一般法*"或"*新法优于旧法*"的原则将存有疑问。同样，自 2021 年 1 月 1 日生效的中国民法通则载有关于个人数据保护和隐私的条款。

In addition, laws that are in the pipeline have an apparent overlap with the DSL, in particular the Personal Information Protection Law ("**PIPL**") for which the second public consultation process is being completed in parallel with that of the DSL.

此外，在审议过程中的法律与数据安全法有明显的重叠，尤其是与数据安全法同时完成第二次向社会公众征求意见程序的《个人信息保护法》（"**个人信息保护法**"）。

We urge the Commission, as a matter of priority, to examine the relevant laws, regulations and guidelines which may overlap with the DSL, and to discuss with the relevant authorities with a view to harmonising the DSL with the other laws,

regulations and guidelines.[4] We recommend refining the scope of the DSL to minimise any overlap with these existing and proposed laws and other data-related laws. In particular, we suggest specifying (or providing ancillary guidance as to):

我们促请法工委优先检视可能会与数据安全法重叠的相关法律、法规和指引，与有关主管机构探讨如何令数据安全法与其他法律、法规和指引保持一致。[4] 我们建议调整数据安全法的范围，尽可能减少与其他数据相关法律的重叠部分。我们尤其建议具体说明下列各项（或提供辅助指引）：

(a) how any inconsistencies with other laws, regulations or guidelines should be resolved; and

如果有与其他法律、法规或指引不一致的情况，将会如何处理；及

(b) how the DSL interacts with other laws, regulations or guidelines.

数据安全法如何与其他法律、法规或指引相互作用。

3. Scope of application

We appreciate that one of the key purposes of the DSL is to safeguard national security. We also recognise the importance of data security in the national security framework. However, the potential reach of the DSL may cause unnecessary burden to financial institutions.

我们认同保护国家安全是制定数据安全法的其中一个主要目的，同时也肯定数据安全对国家安全框架有着举足轻重的作用。然而，数据安全法的潜在涵盖范围可能会对金融机构造成不必要的负担。

Specifically, we believe the DSL casts a net that is too wide, both in terms of:

具体而言，我们认为数据安全法在下列两个方面涉及范围过于广泛：

(a) jurisdictional reach (see paragraph 3.1); and

司法管辖范围（详见第 3.1 段）；及

(b) the definition of key concepts (see paragraph 3.2).

主要概念的定义（详见第 3.2 段）。

3.1. Extraterritoriality

域外法权

The potential reach of the DSL may cause unnecessary burden to international financial institutions. In particular, the DSL covers:

[4] For example, other than the CAC, the PBOC, the China Banking and Insurance Regulatory Commission, and the China Securities Regulatory Commission ("**CSRC**") have also previously issued regulatory requirements relating to data security and data protection.

例如，除国信办外，央行、中国银行保险监督管理委员会和中国证券监督管理委员会（"**证监会**"）先前也曾发布有关数据安全和数据保护的监管规定。

数据安全法的潜在涵盖范围可能会对国际金融机构造成不必要的负担。尤其是数据安全法涵盖：

(a) data processing activities conducted within the PRC ("**PRC Data Activities**"); and

在中国境内开展的数据处理活动（"**中国境内数据活动**"）；

(b) data processing activities conducted by entities or individuals outside the PRC which harm the national security of the PRC, or the lawful interests of PRC citizens or organisations ("**Harmful Non-PRC Data Activities**").

中国境外的组织或个人开展的、损害中国国家安全或中国公民或组织的合法权益的数据处理活动（"**有害的中国境外数据活动**"）。

We strongly urge that the DSL focuses on PRC Data Activities. The provisions in the DSL, whereby any data processing activities conducted outside the PRC which harm the national security of the PRC or the lawful interests of PRC citizens or organisations can trigger Article 2, are too vague and could be interpreted in ways that bring conflicting legal obligations for businesses, which are of serious concern to financial institutions and the wider business community.

我们强烈促请数据安全法围绕中国境内数据活动制定。数据安全法中关于在中国境外开展的任何数据处理活动若损害中国国家安全或中国公民或组织的合法权益的条款可以触发第二条，此规定过于宽泛，可以有多种解读，导致企业的各项法律义务相互冲突，因此金融机构及整个业界极为关注。

Having regard to the strategic importance of data, its need and ability to move across borders, and the number of cloud and other data services provided within the PRC, it is important for financial institutions to understand how the DSL will be applied and enforced in practice, particularly, with respect to foreign entities which do not have physical presence in the PRC.

考虑到数据的战略重要性、跨境需求和能力以及中国境内提供的云端数据和其他数据服务的数量，金融机构有必要了解数据安全法将会如何实际应用和执行，尤其是，针对未在中国境内设立实体机构的境外实体的应用和执行。

More specifically, the application of the DSL to activities of individuals and organisations outside of the PRC is very difficult to apply without clear and objective parameters that can be reasonably assessed by those persons. As drafted, the extra-territorial reach is disproportionate to the potential risk, given there may be very limited PRC nexus (if at all) with data potentially collected and stored wholly outside of the PRC. If extra-territoriality is to be retained in the DSL, the exact scope of Harmful Non-PRC Data Activities must be clarified and we are of the view that unintended harm caused to national/public interests (especially without knowledge) should not be penalised. To the extent that the PRC authorities wish to follow international models on the offering of goods or services into the PRC, it is crucial for businesses to understand the extent of application of these rules and that incidental and inadvertent activities are not unintentionally within its scope. Since the First Review DSL, our membership has emphasised that the implementing rules of the European Union's General Data Protection Regulation ("**GDPR**") should be noted as further discussing how extraterritoriality is aimed only at an intentional, targeted offering of goods or services to individuals in the EU, as opposed to where the provision of goods or services is incidental or inadvertent. As for the First Review DSL, we urge that the DSL must prescribe similar indications to those in the GDPR as to the extent of its extraterritorial application on the offering of goods or services.

具体而言，如果中国境外的个人和组织无法以明确客观合理地作出评估，那么中国境外的组织和个人将难以应用数据安全法于其开展的活动。根据草案，域外应用范围与潜在风险不成比例，并可能与中国的关联非常有限，且可能包含完全在中国境外收集和存储的数据。如果数据安全法要保留域外法权，必须清楚界定有害的中国境外数据活动的明确范围，我们认为，对国家/公众利益的无意损害（特别是在不知情的情况下）不应惩处。倘中国相关机构希望在向中国提供商品或服务方面遵循国际模式，则企业了解这些规则的应用范围至关重要，并确保偶然和无意的活动不在其范围内。自从数据安全法（草案一次审议稿）以来，我们的成员一直强调，应注意欧盟的《通用数据保护条例》（"**GDPR**"）的实施规则的域外法权仅针对有意、有针对性地向欧盟个人提供商品或服务，而不是附带或无意地提供商品或服务。关于数据安全法（草案一次审议稿），我们促请数据安全法须就其对商品或服务提供方面的域外适用范围参照 GDPR 中类似的规定。

Furthermore, as noted above, the DSL's jurisdictional reach also exceeds that of the CSL. We submit that the extra-territorial application of the existing CSL is sufficient to safeguard national security. The very fact of the difference in jurisdictional reach of the DSL and the CSL creates a degree of complexity that has already caused serious concerns among foreign financial institutions. We believe restricting the DSL's extra-territorial application to a smaller scope or one that is commensurate with the CSL, may help alleviate these concerns. In particular, we strongly suggest that areas of law covering a common overall subject matter should be consistent in their application.

此外，如上文所述，数据安全法的司法管辖范围已超过网络安全法的司法管辖范围。我们认为，现行网络安全法的域外应用已足以保障国家安全。事实上，数据安全法与网络安全法之间的司法管辖范围差异会令其应用变得复杂，各境外金融机构均对此深表忧虑。我们认为，将数据安全法的域外应用限制在较小或与网络安全法相同的范围有助缓解此问题。尤其是，我们强烈建议涉及同一类目标整体的法律领域应采用统一的应用标准。

Finally, where certain provisions are *not* intended to apply to data processing activities conducted outside the PRC, the DSL should include an express exclusion, to put the issue beyond doubt. For example, it does not appear practical to require foreign entities to comply with all data security protection obligations set out in Chapter IV of the DSL. It would be preferable to exclude non-PRC Data Activities expressly from those data security protection obligations.

最后，对中国境外开展的数据处理活动不适用的部分条文，数据安全法应作出明确排除，以免除对有关事宜的疑问。例如，要求境外实体履行数据安全法第四章所载列的所有数据安全保护义务看来并不可行。如果能将中国境外数据活动明确排除在该等数据安全保护义务之外，会更为可取。

3.2. Broad definitions of “data” and “data activities”

“数据”和“数据活动”的定义宽泛

The DSL’s scope of application is dictated by the definitions of “data” and “data processing activities”, which, respectively, read as follows:

数据安全法的应用范围取决于“数据”和“数据处理活动”的定义，根据数据安全法：

“Data” refers to any record of information in electronic or non-electronic form.

“数据”是指任何以电子或非电子形式对信息的记录。

“Data processing activities” includes data collection, storage, use, processing, transfer, provision and disclosure.

“数据处理活动”包括数据的收集、存储、使用、加工、传输、提供、披露等行为。

These definitions are very broad. We also strongly believe that inclusive definitions and terms like “including” should be avoided, as they are very difficult to apply in practice and carry a high risk of inconsistent application.

上述定义范围非常宽泛。同时，我们强烈认为，“包括”这类包容性定义和词汇在实际应用时难以付诸实践，且很可能导致应用上的不一致，因此应避免使用这类定义和词汇。

In addition, the definition of “important data” remains outstanding under the DSL, providing for the scope of this data type to be formulated at a later stage. As such, financial institutions and other businesses are unable to understand what “important data” entails and therefore commence operational planning accordingly.

此外，数据安全法下仍未对“重要数据”作出定义，而是规定此数据类型的范围于稍后阶段制定。因此，金融机构及其他企业无法了解“重要数据”的详情，因而无法相应开展经营规划。

To enable financial institutions to formulate effective and practicable compliance measures, we recommend more specificity in the definitions such that the DSL can be fine-tuned to regulate the types of data that will pose real threat to national security.

我们建议数据安全法对有关定义作出更具体的说明，将规制范围明确至真正威胁到国家安全的数据类型，让金融机构能够制定有效且切实可行的合规措施。

4. Data localisation and cross-border transfers of personal information

数据本地化和个人信息跨境传输

Any additional localisation requirements released, as proposed under the DSL for businesses that do not amount to operators of critical information infrastructure, will significantly and arguably disproportionately impact the operation of financial institutions that rely on cross-border transfers of data to facilitate the provision of the best service to customers in the PRC and to ensure the highest level of compliance with anti-money laundering and counter-financing of terrorism laws and regulations through leveraging global service centres. Localisation does not improve data protection. Instead, localisation requirements introduce technical complexity and additional administrative layering into corporate operations, both of which ultimately compromise the effectiveness of cybersecurity and risk management controls.

数据安全法项下对非关键信息基础设施运营者的企业提出的本地化要求，将会对金融机构的运作产生严重并且可以说是不成比例的影响，原因是，这些金融机构在运营时依赖于数据跨境传输，从而为它们通过利用全球服务中心在中国向客户提供最佳服务并确保严格遵守反洗钱和反恐怖主义融资法律法规提供便利。数据的本地化，并不会改进数据保护工作。相反，繁琐的本地化要求，将会为公司的运营带来技术上的复杂性和额外的管理工作，这两者最终都会损害网络安全性和风险管理控制的有效性。

We urge the Commission to consider a more proportionate approach to supervision of exports of data considering the existing laws and regulations already governing this aspect of data use.

鉴于现有的有关数据使用方面的法律法规，我们促请法工委考虑对数据出境采取更为合适的监管方式。

In addition, we specifically recommend significantly narrowing the scope of data that may require prior approval from the competent PRC authorities before that data can be transferred offshore to a foreign law enforcement agency or judicial body.

此外，我们特别建议将可以出境给外国执法机关或司法机构之前须获得中国主管机构事先批准的数据范围大幅缩小。

We recommend that relevant authorities also expressly revise similar existing restrictions (e.g. the CSRC's restriction on the sharing of "any securities business-related data" without CSRC approval) to ensure that the DSL does not contradict existing laws and regulations.

我们建议，相关主管机构同步修改现行的类似限制（例如，证监会禁止在未经其批准的情况下分享“与证券业务活动有关的数据”），确保数据安全法不会与现有法律法规相矛盾。

5. Security system and assessments

安全系统和评估

The Second Review DSL specifically mentions the multi-level protection scheme (“**MLPS**”) on several occasions. However, it is unclear from the overlap between various articles as to whether the intention is to have multiple sets of rules about the MLPS regime.

数据安全法（草案二次审议稿）特别提到在几个情况下的分类分级保护制度（“**分类分级保护制度**”）。但是，从各条款之间的重叠情况看，不清楚其意图是否是就分类分级保护制度制定多套规则。

Any overlap between different provisions in the DSL and existing regulations should be clarified and more details provided to allow financial institutions and other businesses to understanding the obligations imposed on them. This is particularly concerning to our members given the recent increase in scrutiny and enforcement of MLPS in certain locations.

应澄清数据安全法与现有法规的不同条款之间的任何重叠情况，并提供更多细节，让金融机构及其他企业了解对他们的义务。鉴于最近在某些地方对多级数据保护方案的审查和执行有所增加，我们的成员尤其关注这一点。

In respect of the principles underpinning any commercial data classification, we believe that financial institutions and other businesses should be permitted to lead in determining the appropriate classification levels for data under their control, taking a risk-based approach and protecting that data accordingly. This would accord with existing guidance on classification and grading of data.

关于支持任何商业数据分类的原则，我们认为，应允许金融机构及其他企业牵头确定其控制下数据的适当分类级别，采取风险导向的方法，并相应地保护这些数据。这将符合现有的数据分类和分级指引。

On a related issue, Article 23 of the DSL refers to the State establishing a data security review system relating to national security reviews of data processing activities. However, there is insufficient information to enable financial institutions

to properly assess this review's impact on their business operations. We recommend that the Commission provides as soon as possible more details on what the data security review system will entail and how it will be implemented.

在一个相关问题上，数据安全法第二十三条规定国家建立数据安全审查制度，对数据处理活动进行国家安全审查。但没有足够信息使金融机构能够适当评估此种审查对他们的业务经营的影响。我们建议法工委尽快就数据安全审查制度的内容及其如何实施提供更多细节。

Similarly, other data risk assessments are introduced under Article 29 without clarity on the triggering events for a financial institution or other businesses to conduct data risk assessments or how such assessments are fulfilled. Our members believe that financial institutions already have sophisticated risk assessment procedures in place under existing rules, and so should be permitted to decide the frequency of any such assessments themselves.

同样，第二十九条下也引进了其他数据风险评估，但没有明确金融机构或其他企业需要进行数据风险评估的事件或如何进行这些评估。我们的成员认为在现有规则下，金融机构已制定了完善的风险评估程序，因此应允许金融机构自行决定进行任何该等评估的频率。

Part B Specific comments on each article

乙部　有关各条款的具体意见

In addition to the comments raised in **Part A**, we summarise in the table below our comments and recommendations with respect to each article in the DSL.

除**甲部**的意见外，下表概述我们有关数据安全法各条款的意见和建议。

Article 条款	Comments 意见	Recommendations 建议
Chapter I General Provisions **第一章 总则**		
2	Our key concern on this article remains in the Second Review DSL in that we believe that extra-territoriality should be limited to the maximum extent possible. See our comments in paragraph 3.1 in **Part A**. The first paragraph of Article 2 clearly states that the DSL applies to all PRC Data Activities. The second paragraph raises additional ambiguity. It does **not** expressly state that DSL will apply to non-PRC Data Activities. Instead, it merely states that Harmful Non-PRC Data Activities will be subject to legal liability. The second paragraph may indicate some extra-territorial jurisdiction over non-PRC Data Activities (eg to investigate whether they are harmful to the PRC's national security). We submit that the current drafting is too vague, and Article 2 could be interpreted in ways which result in conflicting legal obligations with respect to non-PRC Data Activities for financial institutions. As for the First Review DSL, this has caused serious concerns amongst international financial institutions.	(a) **Article 2 in general** We urge the Commission to re-consider and re-examine the existing National Security Law, CSL, Archive Law and other regulations, and whether the relevant authorities can rely on them to effectively manage and regulate Harmful Non-PRC Data Activities. Overlaps with any existing law should be minimised. (b) **Imported data** We recommend expressly clarifying that data processing activities relating to data that is imported into the PRC for processing and re-exported without co-mingling with PRC data are outside of the scope of the DSL. Such clarification was made in the Information Security Technology - Guidelines for Cross-Border Data Transfer Security Assessments issued by the National Information Security Standardisation Technical Committee in August 2017. Without this clarification, financial institutions will be discouraged from using enterprises in the PRC as outsourcing hubs, leading to lose of revenue-generation and job opportunities to the Chinese economy. (c) **Second paragraph of Article 2** We urge that the DSL focus on PRC Data Activities, and any investigation

		or enforcement powers should not cover non-PRC Data Activities because: • the question of whether non-PRC Data Activities are harmful to the PRC's national security or public interest are likely to be determined through hindsight. Prospective assessments of this are very difficult in practice without detailed parameters and guidance; and • where certain non-PRC Data Activities cause subsequent *unintentional* harm to national security or public interest, there may be an inadvertent result of finding a breach of the DSL without any intent to that effect (*mens rea*). In addition, since the First Review DSL, our membership has further emphasised that the implementing rules of the GDPR should be noted as further discussing how extraterritoriality is aimed only at an intentional, targeted offering of goods or services to individuals in the EU, as opposed to where the provision of goods or services is incidental or inadvertent. As for the Second Review DSL, we urge that the DSL must prescribe similar indications to those in the GDPR as to the extent of its extraterritorial application on the offering of goods or services. We suggest refining the test such that it would require at least some degree of intention to conduct Harmful Non-PRC Data Activities in order to be subject to any investigation or enforcement. Please refer to our recommendations in paragraph 3.1 of **Part A** and our comments on Article 34 in this **Part B**.

第二条	在数据安全法（草案二次审议稿）中，本条我们关心的主要问题是域外法权，我们认为应尽可能限制域外法权的范围。详见我们在**甲部**第 3.1 段的意见。 第二条第一段明确指出数据安全法适用于一切中国数据活动。 第二段的措词更加模糊，其中并无明确指出数据安全法将应用于中国境外数据活动，只是表示会依法追究有害的中国境外数据活动的法律责任。 第二段可能包含部分对中国境外数据活动的域外司法管辖权（如调查有关数据活动是否损害中国国家安全）。 我们认为，目前的草案过于宽泛，第二条可以不同方式解读，导致境外金融机构开展中国境外数据活动须承担的法律义务相互冲突。在数据安全法（草案一次审议稿）中，国际金融机构对此有很大忧虑。	(a) **第二条整体** 我们促请法工委重新考虑和检视现行国家安全法、网络安全法、档案法和其他法规，并重新考虑和检视相关主管机构是否可依赖上述法律法规有效管理和监管有害的中国境外数据活动，尽可能避免数据安全法与现行法律重叠。 (b) **入境数据** 我们建议明确澄清，入境中国用于加工及再出境并且并未与中国境内数据混合的数据的数据处理活动不属于数据安全法范畴之列。此项澄清已在全国信息安全标准化技术委员会于 2017 年 8 月发布的“信息安全技术- 数据出境安全评估指南”征求意见稿中有所体现。若无此项澄清，金融机构将倾向于不再使用中国境内企业作为其外包机构，这将使得中国经济流失一定的创收与工作机会。 (c) **第二条第 2 段** 我们促请数据安全法应围绕中国数据活动制定，有关调查或执法不应覆盖中国境外数据活动，理由如下： • 就中国境外数据活动是否损害中国国家安全或公共利益而言，通常是事发之后才可确定。如缺少详细参数和指引，在实践中极难进行前瞻性评估；及 • 如果若干中国境外数据活动在进行之后*无意中*损害了国家安全或公共利益，则有关活动可能在无意间违反了数据安全法（无犯罪意图）。 自数据安全法（草案一次审议稿）以来，我们的成员进一步强调，应注意到 GDPR 的实施细则的域外法权仅针对有意、有针对性地向欧盟境内个人提供商品或服务的情况，而非针对附

		带或无意地提供商品或服务的情况。就数据安全法（草案二次审议稿）而言，我们建议数据安全法须就其对商品或服务提供方面的域外适用范围参照 GDPR 中类似的规定。 我们建议调整标准，需要至少有一定程度的意图进行有害的中国境外数据活动，才会展开调查或执法。 请参阅我们在**甲部**第 3.1 段和**乙部**有关第三十四条的建议。
3	The definitions of “data”, “data processing” and “data security” are too broad. In particular, the definition of “data processing” can potentially cover all aspects of commercial activities involving data.	We recommend refining the definitions such that including “impacting national security” or “safeguarding national sovereignty” to the definitions of “data”, “data processing” and “data security” so as to refine the DSL’s scope of application. Please also refer to our recommendations in paragraph 3.2 of Part A
第三条	“数据”和“数据处理”的定义过于宽泛。 尤其是，“数据处理”的定义可能包含涉及数据的商业活动的各个方面。	我们建议修改有关定义，以达到下列目的： 在“数据”和 “数据处理”的定义中加入“影响国家安全”或“捍卫国家主权”，以调整数据安全法的应用范围；及 亦请参阅我们在**甲部**第 3.2 段的建议。
4	We understand that the State will establish the “data security governance system” and promote the enhancement of “data security protection capabilities”. Members understand this to refer to a governance framework among governmental authorities, departments and regulators, in the manner set out in Articles 6 and 7.	We recommend clarifying that Article 4 applies only to governmental authorities, departments and regulators as described in Articles 5 and 6, rather than to private entities such as financial institutions.
第四条	我们理解国家将建立“数据安全治理体系”，并提高“数据安全保障能	我们建议明确第四条仅适用于第五条和第六条项下的政府机构、部门和监

	力”。我们的成员理解这意指第六条和第七条项下的政府机构、部门和监管者构成的监管框架。	管者，而不包含非公共部门,例如金融机构。
6	It appears from this article that the Central National Security Commission (“**CNSC**”) will be the central policy maker for data security. Our general understanding is that the Central National Security Commission primarily focuses on political security and intelligence. This is quite different from the existing regulatory landscape with respect to financial institutions’ use of data. It is unclear how the role of the relevant national security authorities will impact the overall regulatory culture and framework for day-to-day data regulatory matters.	(a) **Role of CNSC** We suggest clarifying the roles and responsibilities of the CNSC and the national cyber space authority (which is responsible for the comprehensive coordination of network data security and related supervision work according to Article 7 of the Second Review DSL). In particular, we recommend clarity as to whether this means the CNSC will be responsible for the comprehensive coordination of the security and related supervision of non-networked data. Please clarify to what extent this change in regulatory landscape would impact financial institutions, for example: • whether new rules or regulations will be issued by CNSC; and • whether financial institutions need to actively monitor for any new rules issued by the CNSC. (b) **PBOC as lead regulator for financial sector** As financial institutions are highly regulated in many aspects, in circumstances where the DSL has implications for the financial sector, we recommend that any additional rules or regulations to be imposed on financial institutions should be at least reviewed, and preferably issued, by PBOC, an authority that would know the intricacies of the existing and new rules.

		Please also refer to our recommendations in paragraph 1 of **Part A**.
第六条	从本条条款上看，中央国家安全委员会（“**国安委**”）将作为数据安全的中央政策决策人。根据我们的普遍理解，中央国家安全委员会主要负责政治安全和情报工作。 这与目前的金融机构数据使用监管框架相去甚远。 有关国家安全机构所发挥的作用将如何整体影响与日常数据监管事项有关的监管文化和框架尚不明确。	(a) **国安委的作用** 我们建议厘清国安委和国家网信部门的作用和职责（根据数据安全法（草案二次审议稿）第七条，国家网信部门负责统筹协调网络数据安全和相关监督工作）。尤其是，我们建议清楚说明这是否意味着国安委将负责统筹协调非网络相关数据的安全和相关监督工作。 建议说明此监管架构的变动对金融机构的影响有多大，例如： • 国安委是否会出台新规则或法规；及 • 金融机构是否需要主动监测国安委颁布的新规则。 (b) **央行作为金融行业的牵头监管机构** 因为金融机构在各方面受到严格监管，考虑到数据安全法会相应影响到金融行业，由于央行比较了解现行和任何新订规则的各种错综复杂的关系，我们建议，针对金融机构实施的任何额外规则或法规至少须经过央行审阅，且最好由央行颁布。 亦请参阅我们在**甲部**第 1 段的建议。
7	This article provides that the following authorities are responsible for the supervision of data security: (a) regulatory bodies of specific sectors including finance; and (b) public security authorities and national security authorities. This raises concerns about inconsistent interpretation and enforcement of the DSL by the different authorities.	We make the following recommendations here: (a) **One centralised regulator** If the DSL has implications for the financial sector, we recommend that data processing by financial institutions should be supervised by a single regulator (or at least one *primary* regulator) to ensure consistent interpretation and enforcement of the DSL requirements.

		We recommend that the lead regulator for financial institutions should be the PBOC for the reasons set out in our comments on Article 6, consistent with our comments in paragraph 1 of **Part A**. (b) **Involvement of local governments** Please clarify the local governments' involvement as referred to the first paragraph (e.g. whether they will be making rules or regulations), and how they will interact with other relevant authorities. We submit that some financial institutions have branches and places of business in multiple provinces in the PRC. It would pose practical difficulties to them if they are required to comply with different rules in respect of the same piece of data which may be used in multiple locations. (c) **The role of public security bodies and national security bodies** The DSL should expressly clarify that public security bodies and national security bodies may enforce the DSL in case of an infringement, but they should not be responsible for the day-to-day supervision of financial institutions. The sectoral regulator should act as the primary regulator. (d) **The role of relevant authorities for national cybersecurity and information** The last paragraph positions such relevant authorities for national cybersecurity and information (which may include CAC) as coordinator for electronic or network data. Please clarify their role, e.g. whether such authorities will be involved in enforcing the DSL. We reiterate that

		the sectoral regulator should be the primary regulator with respect to the sector it covers. It should also continue to be responsible for ensuring consistency between its own sectoral rules.
第七条	本条规定以下机构承担数据安全监管职责： (a) 金融业等特定行业的监管部门；及 (b) 公安机关和国家安全机关。 我们担心此规定会导致不同机构对数据安全法的解释和执行不一致。	我们的建议如下： (a) **单一的中央监管机构** 在数据安全法影响到金融行业的情况下，我们建议由单一的监管机构（或至少指定一个*主要*监管机构）监督金融机构的数据处理，确保对数据安全法相关规定的解释和执法保持一致。 出于我们在有关第六条的意见中给出的相同理由，我们建议由央行担任金融机构的牵头监管者，这与我们在**甲部**第 1 段的意见一致。 (b) **地区政府的参与** 就第一段所述的地区政府的参与作出清晰说明（如有关政府是否会制定规则或法规等），并说明地区政府将如何与其他相关主管机构相互合作。 部分金融机构在中国多个省份设有分支机构和营业地点，我们认为，如果该等金融机构须就同一项数据在不同地区遵守不同规则，在实际执行中将面临困难。 (c) **公安机关和国家安全机关的作用** 数据安全法应明确指出，公安机关和国家安全机关会对任何违反数据安全法的行为执法，但不负责对金融机构的日常监督。主要监管机构应由行业监管机构担任。 (d) **国家相关网信机关的作用**

		最后一段指出国家相关网信机构（可能包括国信办）负责电子或网络数据的协调工作。请清楚说明有关机构的作用，如有关机构是否会参与数据安全法的执行等。我们重申，主要监管机构应由相关行业的行业监管机构担任。行业监管机构亦须继续负责确保其各项行业规则保持一致。
10	We note that the Second Review DSL includes a specific proposal for industry associations and other trade bodies to develop codes of conduct on data security, strengthen industry self-discipline and guide their members to improve standards.	While financial institutions generally favour self-regulation in industry-specific tenets of operation such as data management, more guidance will be needed for foreign chambers of commerce and other broad-discipline organisations in the financial services sector to understand what role is expected of them under these new requirements. However, it may not be necessary to include any stipulations in this regard in the DSL as industry practice and self-regulation should be a market-driven, voluntary mechanism.
第十条	我们注意到，数据安全法（草案二次审议稿）包含一项具体提议，要求行业协会与其他行业组织制定数据安全行为规范，加强行业自律，指导其会员加强数据安全保护。	虽然金融机构通常倾向于在行业特定的运作原则方面实行自我监管，例如数据管理，但外国商会和金融服务部门的其他自治组织仍需要更多的指导，以了解它们在这些新要求下应发挥何种作用。 但是，由于行业惯例和自我监管应是基于市场驱动的自愿机制，可能并没有必要在数据安全法中纳入这方面的细致规定。
11	It appears that the DSL seeks to encourage cross border data sharing provided that it is legitimate and safe.	We recommend the Commission to communicate with financial regulators, to reflect this policy to encourage cross border data sharing. We note that the State will participate in the formulation of international regulations and standards on data security to facilitate cross border data transfer. We recommend that any

		such new regulations should make clear: (a) that the PRC supports the free flow of data across borders; (b) the scope of cross border data transfer that will be allowed (including any restrictions on the types of data or other caveats as were agreed as recently as November 2020 with the agreement of the Regional Comprehensive Economic Partnership including commitments on cross-border transfers of data in Chapter 12); (c) whether cross-border transfers of certain types of data will be subject to conditions. In particular, financial institutions are required to disclose data for anti-money laundering and counter-terrorism financing purposes, both within their corporate groups and externally to comply with regulatory obligations. We suggest that this type of cross-border data transfer should not be subject to any conditions. See also our comments on Article 35 of **Part B**; (d) the procedural requirements (e.g. whether entities need to undertake a data security self-assessment before conducting cross-border data transfer); and (e) the relevant regulator for supervising the financial institutions in relation to cross-border data transfer activities. As a general principle, we suggest that international standards with respect to cross-border data transfers be taken into account when designing these cross-border data controls to facilitate the secure flow of data.

		Please also refer to our recommendations in paragraph 4 of **Part A**. Further, we recommend the Commission to reconcile Article 11 with Article 35, including specifying the types of data which financial institutions may transfer out of the PRC without prior approval of the relevant authorities (the current formulation under the Second Review DSL, as for the First Review DSL, simply uses the broad terms of ALL "data"). In addition, we suggest that the Commission clarifies that any preferential policies in respect of cross-border data transfers released by authorities of free trade zones or special economic areas at provincial or municipal levels will remain valid.
第十一条	从条款上看，数据安全法鼓励合法安全的跨境数据分享。	我们建议法工委与金融监管机构沟通以反映这项鼓励跨境数据分享的政策。 我们注意到，国家将参与数据安全相关国际规则和标准的制定，促进数据跨境流动。我们建议，任何有关新规则应清晰说明下列各项： (a) 中国支持数据跨境自由流动； (b) 允许数据跨境传输的范围（包括对数据类型的任何限制或者最近于 2020 年 11 月商定的其他附加说明，该附加说明系《区域全面经济伙伴关系协定》所载（包括第十二章关于数据跨境传输的承诺））； (c) 部分类型的数据跨境传输是否须遵守特定条件。尤其是，金融机构在其企业集团内部和外部都要遵守监管义务，为反洗钱和打击恐怖分子资金筹集目的披露数据。我们建议，不应对这类的数据跨境传输施加任何条件。亦请参阅我们在**乙部**就第三十五条提出的意见；

		(d) 程序要求（例如实体在进行跨境数据传输前是否需要进行数据安全评估）；及 (e) 负责监督金融机构数据跨境传输活动的相关监管机构。 作为一般性原则，我们建议在设置有关跨境数据管制时，应参考跨境数据传输的国际标准，以促进数据的安全流动。 亦请参阅我们在**甲部**第 4 段的建议。 此外，我们建议法工委确保第十一条与第三十五条保持一致，包括列明在无须有关主管机构批准的情况下金融机构可向中国境外传输的数据类型（此为数据安全法《草案二次审议稿》的表述，而数据安全法（草案一次审议稿）中仅使用了广义的表述——所有“数据”）。此外，我们建议法工委须明确省级或市级自由贸易区或经济特区发布的数据出境传输相关的任何优惠政策仍将继续有效。
12	NA	Please provide details of the “relevant authority” for the purpose of reporting any breach of DSL.
第十二条	不适用	请提供接收违反数据安全法举报的「有关部门」的详情。
Chapter II Data Security and Development **第二章 数据安全与发展**		
16	We note that the relevant administrative departments in the State Council are responsible for formulating standards concerning standards relating to data development, data technologies and data security. Implementation of global standards is crucial to developing the PRC financial market and attracting foreign investors. The potential differences in legal and regulatory requirements regarding data security across	We make the following recommendations here: (a) **Adopting existing international standards and best practices** We are of the view that these standards should recognise and adopt relevant international standards as much as possible. If full adoption is not possible, the standards should be aligned with relevant international standards, and formulated having regard to overseas practices to ensure the efficient flow of data and

	different sectors and different regions in the PRC is an area of focus and concern which may deter investment.[5] This is particularly relevant to multinational financial institutions which may need to use, process or store data in multiple locations. If the standards are not compatible with international standards, it may result in conflicting legal and regulatory obligations, which will pose significant challenge to multinational financial institutions.	compatibility in practice, particularly in the context of cross-border financial activities. We recommend setting out the details by way of core principles of data security which allow each organisation to adopt a risk-based approach to address the specific risks it faces. (b) **Proposed amendments** We recommend amending Article 16 as follows: *"The State advances the construction of data development and use technology and data security standards systems. The State Council administrative department for standardisation and relevant State Council departments will, according to their respective duties and responsibilities, organise the formulation and timely revision of standards concerning data development and use technologies and products and security-related standards~~. The State~~ following the principles of transparency, openness, impartiality and consensus, effectiveness and relevance, and coherence. The State creates an open and inclusive standard setting environment and supports enterprises, social organisations and educational and scientific research institutions, institutions of higher*

[5] Based on the "Study on Trading and Clearing Trends in Derivatives Markets" released by FIA in March 2020 (available at: https://www.fia.org/resources/fia-greenwich-associates-release-new-derivatives-market-research (English version only)), the industry's top request in terms of the changes they would like to see from policymakers is to lower barriers for cross-border trading and clearing (see pages 6 and 7). The interest in the PRC markets by U.S. and European firms only adds to the importance of efficient cross-border operations. According to the study, 29% of respondents stated they are already active in Chinese futures, 20% are planning to enter the market soon, while 18% are exploring opportunities there. This study pre-dates the global spread of the Covid-19 pandemic, but it gives an indication of the strong interest in the PRC market by industry participants.

根据 FIA 于 2020 年 3 月发表的《衍生工具市场交易和结算趋势研究》（网址：https://www.fia.org/resources/fia-greenwich-associates-release-new-derivatives-market-research（该研究报告仅有英文版）），行业最期待的变化是政策决策者能够降低跨境交易和结算的门槛（详见该研究报告第 6、7 页），而欧美公司对中国市场的兴趣更会凸显高效跨境运作的重要性。根据研究报告，29%的调查对象称他们已积极参与中国期货市场，20%的调查对象正计划于不久的将来进入市场，另有 18%的调查对象正在有关市场发掘机会。尽管此研究报告的发表时间早于新冠肺炎的全球爆发，但仍可从报告中看出业界参与者对中国市场具有的强烈兴趣。

		education to participate in the formulation of standards." (c) **Involving foreign entities in the drafting process** We recommend the government build standards with participation on a voluntary basis by relevant stakeholders, including foreign entities, to ensure practicality and effectiveness. We expand on this process in paragraph 1 of **Part A**. (d) **Uncertainty about the legal effect of industry standards** Please clarify the nature of the standards formulated pursuant to Article 16 (e.g. mandatory requirements in rules or regulations, or industry recommended standards), and the implementation plan for the standards.
第十六条	我们注意到，制定数据开发、数据技术和数据安全相关标准，是由国务院有关行政部门负责。 此外，国际标准的实施对发展中国金融市场和吸引外资进入十分关键。中国不同行业和地区在数据安全相关法律和监管规定方面的潜在分歧势必会引发关注和忧虑，有碍投资进入。[6] 需要在不同地区使用、处理或存储数据的跨国金融机构尤为如此。如果有关标准不能与国际标准挂钩兼容，可能会导致法律和监管义务冲突，对跨国金融机构构成严峻挑战。	我们的建议如下： (a) **采用现行国际标准和最佳惯例** 我们认为，有关标准应尽可能承认和采用相关国际标准。如果不能完全采纳国际标准，该等标准也应该与相关国际标准具有相当一致性，其制定应考虑到海外惯例，确保数据有效流动以及在惯例上相容（尤其是在进行跨境金融活动时）。 我们建议以数据安全核心原则的方式作出详细说明，让各组织机构能够采用风险导向方法处理其面临的特定风险。 (b) **建议修订** 我们建议对第十六条作出如下修订： *"国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，秉持透明、公开、公正与共识、有效与相关和一致性的原则组织制定并*

		适时修订有关数据开发利用技术、产品和数据安全相关标准。国家致力于创造一个公开、具包容性的标准制定环境，支持企业、社会组织以及教育与科学研究机构、高等学校参与标准制定。” (c) **境外实体参与起草程序** 我们建议政府在制定标准时，应允许包括境外实体在内的利益相关者自愿参与，以确保有关标准切实可行，行之有效。我们对有关程序的建议在**甲部**第 1 段详述。 (d) **行业标准的法律效力尚不明确** 请说明根据第十六条制定的标准的性质（例如是属于规则或法规的强制规定，还是属于行业推荐标准等），并说明有关标准的实施计划。
17	We welcome the PRC's support for specialised agencies to provide services in respect of data security monitoring, assessment and certification.	Please clarify: (a) whether these specialised agencies will be required to be certified by the relevant authorities; (b) if so, the specific criteria for the certification, and the timeline for obtaining such certification; and (c) Whether a data security risk assessment needs to be performed by the specialised agency. We submit that self-assessment using a financial institution's independent internal qualified functions (eg risk management or audit) should suffice. [6] See also our

[6] For example, a number of international financial institutions will already have adopted international cybersecurity principles such as the so-called three lines of defence model. Any internationally qualified professional within an internal department should be adequately qualified to conduct a self-assessment because he or she will have a better understanding of the institution's hierarchy and can independently report to the risk and audit bodies of the institution.

譬如，许多国际金融机构已采纳了国际网络安全原则，例如所谓的三重防线模式。在内部部门工作的国际合资格专业人士应拥有足够资质进行自我评估，因为他/她更了解机构的体系并且能够独立向机构的风险及审计部门汇报工作。

		recommendation in relation to Article 21.
第十七条	我们欢迎中国支持专业机构提供数据安全检测、评估和认证服务。	请说明： (a) 有关专业机构是否须获相关主管机构认证； (b) 如是，请列明认证的具体标准和取得有关证书的所需时间；及 (c) 数据安全风险评估是否须由专业机构进行。我们认为，由金融机构内部的独立合资格部门（如风险管理部或审计部）进行自我评估已经足够 [6]。请同时参阅我们有关第二十一条的建议。
18	NA	We note that Article 18 provides a policy direction. We share our view that: • the data transaction market should not be overly regulated, as it would be burdensome for firms engaging in data transaction activities, and detrimental to development of the market and business interests. We recommend promoting and incentivising voluntary sharing at the initial stage; and • a foreign entity should be permitted to participate in the data transaction market as a data transaction intermediary, a data receiving party and a data providing party. This would help develop the market.
第十八条	不适用	我们注意到，第十八条提供了政策方针。 我们认为： • 数据交易市场不应受到过度监管，因为这会对从事数据交易活动的公司造成沉重负担，不利于市场发展，损害商业利益。我们

		建议在初始阶段应促进和鼓励自愿分享；及 • 应允许境外实体作为数据交易中介机构、数据接收方和数据提供方进入数据交易市场。这有助于市场发展。
Chapter III Data Security Systems **第三章 数据安全制度**		
20	We note that the Second Review DSL specifically mentions the MLPS on several occasions. Comments on the First Review DSL highlighted that references to classification of data and related protection systems would seem to reference the MLPS provided for under article 21 of the CSL, so this clarification that this is the Commission's intention is welcomed from the perspective of operational planning certainty. While we are generally of the view that the tiered data security system is an important part in safeguarding data security, having multiple sets of rules on the MLPS regime (if that is the intention of different references in this article and also Article 26) could cause contradiction or other confusion for businesses. Furthermore, the references are vague and lack details on how the tiered data security system(s) will operate.	(a) **Confusion on Articles 20 and 26** We recommend that any potential for overlap and therefore confusion as a result of similar concepts being introduced in each of Articles 20 and 26 is resolved. Article 20 requires the State to establish a MLPS for data, while Article 26 suggests that the existing MLPS established under the Cybersecurity Law should be the baseline governance framework for management of data processing activities. It is unclear whether the intention is that both articles refer to the same MLPS regime. If not, there is a risk of creating two apparently similar classification regimes for managing data-related risks, which may create unnecessary complexity. We suggest that the Commission considers aligning Articles 20 and 26 to build on the existing MLPS regime, and amend Article 20 accordingly to confirm that the implementation of multi-level protection for data will be in alignment with the MLPS required under the CSL. **(b) More detailed guidance required** Once it is ensured that there is no contradiction or other confusion caused by the co-existence of multiple sets of rules on one regime, we recommend detailed guidance in respect of the level of protection required and the enforceability of tiered data security system is

		released or, ideally, existing guidance can be refined and (where appropriate) supplemented in consultation between industry regulators and businesses and relied on to avoid co-existence with another separate regime (see (c) below). This would enable financial institutions to formulate and implement appropriate measures to ensure compliance. (c) **Risk-based data classification** We refer to the guidance on classification and grading of data for security and futures industry issued by CSRC which is a non-mandatory recommended industrial standard. This CSRC guidance provides for a multi-level data protection scheme conducted at an industry-specific level. Industry supports sound data governance practices in line with international standards. For commercial data classification, financial institutions and other businesses should be permitted to lead in determining the appropriate classification levels for data under their control, taking a risk-based approach and protecting that data accordingly. Furthermore, financial institutions are subject to various regulations and any additional standardisations and categorisations should be avoided so as to reduce possible overlaps and inconsistencies.
	我们注意到，数据安全法（草案二次审议稿）有好几处特别提到分类分级保护制度。数据安全法（草案一次审议稿）的相关意见强调了，凡提及数据分级及相关保护制度之处似乎可以援引到网络安全法第二十一条规定的分类分级保护制度，因此从操作规划确定性的角度来说，该等符合法工委	(a) **第二十条与第二十六条的混淆** 我们建议解决因第二十条和第二十六 条引入类似概念而导致的任何可能的重叠和混淆。 第二十条要求国家为数据建立分类分级保护制度，而第二十六条则建议，根据网络安全法建立的现行分类分级保护制度应当是管理数据处

	意图所作出的关于数据分类分级保护方面的进一步澄清是受欢迎的。 尽管我们基本上认为，数据安全分级制度是保护数据安全的重要一环，但是在分类分级保护制度上设置多套规则（如果这本来就是本条及第二十六条的目的的话）可能会导致从商业角度来看的矛盾或其他混乱。再者，有关数据安全分级制度将如何运作的描述十分模糊，不够详细。	理活动的基本治理框架。 目前尚不清楚是否这两条规定指向的是同一分类分级保护制度。 如果不是这样的话，就有可能为管理数据相关风险而建立两个明显相似的分类分级制度，这可能会导致不必要的复杂性。 我们建议法工委基于现行分类分级保护制度使第二十条和第二十六条保持前后一致，并相应修订第二十条，以确认实施数据多层保护符合网络安全法所要求的分类分级保护制度。 **(b) 需要更详细的指引** 一旦确保在一个制度上共存多套规则不会产生矛盾或其他混乱，我们建议就所需保护的级别和数据安全分级制度的可执行性发布详细指引，或者理想的做法是，现有指引经过行业监管机构与企业磋商之后可以进行改进及（如适用）补充，从而避免与其他单独的制度共存（见下文(c)款）。这将令金融机构能够制定和实施适当的措施，确保合规。风险导向的数据分级分类 据我们所知，证监会颁布的《证券期货业数据分类分级指引》是非强制性的行业建议标准。此证监会指引提供了面向特定行业的多级数据保护方案。行业支持符合国际标准的稳健的数据治理做法。对于商业数据分类分级，金融机构及其他企业应获准率先确定其所控制数据的适当分类、采取以风险为导向的方法并相应地保护数据。此外，金融机构须遵守若干法规，因此，应避免任何额外标准和分类，以降低范围重叠和不一致的可能性。 **(c) 风险导向的数据分级分类** 据我们所知，证监会颁布的《证券期货业数据分类分级指引》是

		非强制性的行业建议标准。这一证监会指引提供了面向特定行业的多级数据保护方案。行业支持符合国际标准的、稳健的数据治理做法。对于商业数据分类分级，金融机构及其他企业应获准率先确定其所控制的数据的适当分类、采取风险导向的做法并相应地保护数据。 此外，考虑到金融机构须遵守若干不同法规，因此，应尽量避免任何额外的标准和分类，以减少可能的范围上的重叠和不一致性。
	There may be inconsistent definitions of "important data". The DSL does not define "important data". Instead, the State shall formulate a catalogue of "important data", to be then used by relevant regions, departments, industries and sectors. The formulation of the catalogues across different regions and industries may differ. This inconsistency will cause practical difficulty in compliance, particularly, for financial institutions with branches and places of business in multiple provinces in the PRC, as they may need to store and use the data on both a localised and a centralised basis.	(a) **Define "important data" in the DSL** We submit that the definition of "important data" should be consistent across data processing activities, regardless of the location and industry in which the data is used. We also request the Commission to clarify whether "important data" will form part of the "controlled categories" referred to in Article 24. (b) **Industry-specific catalogue prevails over location-specific catalogue** If the Commission does not agree with having one single definition of "important data", we suggest that the DSL should expressly provide that the definition or catalogue of "important data" issued by sectoral regulatory authorities prevail over that issued by local governments. We believe each sector or industry has different practices and concerns with respect to data use and suggest PBOC centrally take the lead and develop the important data catalogue for the financial sector as a whole. The relevant regulators are in the best position to formulate the scope of "important data" so as to achieve the purpose of safeguarding national

		security and public interest while minimising impact on businesses. The relevant regulators should also provide guidance on how to deal with data which falls within the ambit of more than one industry-specific catalogue. (c) **Involving market participants in drafting of the definition of "important data"** We request relevant authorities to actively seek the views of market participants and involve them in the drafting process when formulating the "important data" definition or catalogue. Please also refer to our recommendations on having the PBOC as the lead and co-ordinating regulator for financial institutions in paragraph 3.2 of **Part A**. This is particularly important as Articles 26 and 29 of the DSL impose various data security protection obligations on financial institutions including their responsible persons and management bodies. See also our comments on Article 26. (d) **How the concept of "important data" interacts with previous draft regulations and existing law** We refer to: • the draft Guidance on Security Assessment – Guidance for Cross border Data Transfer (2017) issued by National Information Security Standardisation Technical Committee ("**Guidance**"); and • the draft Financial Data Security – Guides of Data Security Classification (2020) issued by PBOC ("**Guides**"). The Guidance and the Guides provide details on the meaning of "important data". Please clarify whether or how

		the Guidance and the Guides may impact the tiered data security system and that such non-mandatory guidelines remain recommendatory only. We also suggest that the meaning of "important data" referred to in the Cybersecurity Law and the DSL's "important data" should align.
	"重要数据"的定义可能存在分歧。 数据安全法并无界定"重要数据"，但是国家应制定"重要数据"目录，以供相关地区、部门以及各行各业使用。不同地区、不同行业指定的保护目录可能互不相同。目录不一致会导致在中国多个省份设有分支机构和营业地点的金融机构可能需要分别按照地区和集中基准存储和使用数据，在合规方面的实际运作层面面临困难。	(a) **数据安全法对"重要数据"的定义** 我们认为，不论使用数据的地点与行业，"重要数据"的定义应在整个数据处理活动中保持一致。 我们请求法工委阐明「重要数据」是否属于第二十四条所述的「管制物项」类别。 (b) **特定行业目录优于特定地区目录** 如果法工委不同意赋予"重要数据"单一定义，我们建议数据安全法应明确规定行业监管机构公布的"重要数据"的定义或目录优于地区政府公布的定义或目录。 我们认为，各行业或领域对数据使用的惯例和关注点互不相同，并且建议央行应牵头为整个金融行业制定重要数据类别。有关监管机构是最适合的机构就"重要数据"的含义制定范围，从而达到保护国家安全及公共利益，和减少对商业造成影响的目的。有关监管当局还应该提供相关指引，说明应如何处理涉及多个行业特定目录的数据。 (c) **邀请市场参与者参与起草"重要数据"的定义** 我们请求有关当局积极寻求市场参与者的意见，邀请他们参与制定"重要数据"定义或目录的起草程序。请同时参阅我们在**甲部**第3.2段作出的有关指定央行为金

		融机构的牵头协调监管机构的建议。 这对数据安全法第二十六、二十九条尤为重要，有关条款对金融机构（包括其责任人和管理机构）施加了各种数据安全保护义务。请同时参阅我们对第二十六条的有关意见。 (d) **“重要数据”概念与先前的法规草案和现行法律的关系和相互作用** 我们谨此提述： • 全国信息安全标准化技术委员会颁布的《数据出境安全评估指南（草案）》(2017 年) (“**评估指南**”)；及 • 央行颁布的《金融数据安全数据安全分级指南（草案）》(2020 年) (“**分级指南**”)。 评估指南和分级指南具体说明了“重要数据”的涵义。请阐明评估指南和分级指南是否会或将如何影响数据安全分级制度并且该等非强制性指引仍仅作为建议。我们还建议，“重要数据”的涵义在网络安全法和数据安全法内应保持一致。
21	The centralised mechanism for data security risk assessment, reporting, data sharing and supervision is likely to impact the operation of financial institutions.	We recommend that compliance by financial institutions with the centralised mechanism should be voluntary at the initial stage. This would facilitate the relevant authorities to review its efficiency and effectiveness. The requirements under the mechanism should not be too onerous, as any such requirements will be detrimental to economic and business interests. In respect of the reporting mechanism, we recommend introducing the concept of a risk-based approach and self-assessment. Such assessment

		should be formulated having regard to the nature, volume and sensitivity of the data. A lead regulator (e.g. PBOC as recommended) could develop best practice guidance together with financial market participants, so that they can give due consideration to issues such as confidentiality, participation in international financial markets, intellectual property and other related legal obligations. Please see the Financial Services Sector Cybersecurity Profile developed by the Financial Services Sector Coordinating Council[7] as an example of a risk-based assessment tool.
第二十一条	集中统一的数据安全风险评估、报告、信息共享和监测机制很大可能会影响金融机构的运营。	我们建议，在初始阶段，金融机构遵守集中统一的机制应以自愿性为基础。 这有助有关主管机构检讨该机制的效率和有效性。 该机制下的有关规定不应过于繁重，否则会损害经济和商业利益。 在报告机制方面，我们建议引入风险导向方法和自我评估的概念。有关评估的制定应考虑数据的性质、数量和敏感度。牵头监管机构（例如我们所建议的央行）可与金融市场参与者共同制定最佳惯例指引，以充分考虑到机密性、参与国际金融市场、知识产权和其他相关法律义务等问题。 有关风险导向评估方法，请参阅美国金融服务行业协调委员会[7]编撰的《金融服务行业网络安全概况》。
23	**(a) Lack of sufficient details** The DSL does not contain sufficient information relating to the data security review system to enable financial institutions to properly	We recommend: • providing more details on what the data security review system will entail and how it will be implemented;

[7] Available at: https://fsscc.org/Financial-Sector-Cybersecurity-Profile. (English version only)
可于以下网址查阅：https://fsscc.org/Financial-Sector-Cybersecurity-Profile（仅有英文版）

	assess its impact on their business operations and their risks.	• restricting the scope of the application of the data security review system such that it can focus on addressing key national security concerns; • clarifying when a data security review will be triggered and what types of "data" or "data activities" will be covered, and who will be qualified to conduct the data security review (e.g. whether the review will be conducted by a relevant authority, or whether a financial institution will be expected to engage independent auditors, or use internal resource to conduct the review); and • that the Commission prepare and make available to all financial institutions a matrix of relevant authorities for each industry and region.
	(a) 缺少具体说明 数据安全法并无载有足够的数据安全审查制度的相关信息，让金融机构无法评估该制度对其业务经营的影响和制度相关风险。	我们建议： • 提供有关数据安全审查制度会造成的影响和在实施方面的更多详情； • 限制数据安全审查制度的应用范围，数据安全审查制度应专注处理关键的国家安全问题； • 列明会触发数据安全审查的情况、数据安全审查所覆盖的"数据"或"数据活动"类型和合资格进行数据安全审查的人员／机构（例如，审查是否由相关主管机构执行，或是否希望金融机构聘请独立核数师或使用内部资源进行审查）；及 • 法工委应为各金融机构编制一份包含各行业和各地区的相关主管机构名单。
	(b) Broad potential application Having regard to the broad definition of "Data Processing activities", we are concerned that this article may lead to	We recommend clarifying how the data security review in this article relates to the "security assessment processes" described in the Cybersecurity Law and the second

	an unintendedly broad interpretation and application.	review draft of the PIPL ("**Second Review PIPL**"), the data security risk assessment (as stated in Article 21), the draft guidelines issued by the CAC and industry standards. We suggest that a financial institution should be exempted from the data security review if it has conducted a security assessment process in the past year. We recommend clarifying the nature of this national security review in the context of data processing activities. There are already a number of existing and proposed mechanisms in place for review of data processing activities, such as the cross-border security assessments required under Article 30 and under the CSL, and, to maintain business efficiency, any duplication of processes should not be created. Implementing rules clearly setting out the triggers for a review and the scope and process for the review (including the statutory timeline) should be released as soon as possible. Where it is feasible to include a decision appeal process, this should be incorporated for the purpose of accountability under the principles of the rule of law. At a minimum, a channel should be implemented to share with the relevant parties disclosable information as to why the decision was made, so as to provide transparency that all important facts have been considered in the decision.
	(b) 潜在应用范围较广 鉴于"数据处理活动"的宽泛定义，我们担心本条可能会在无意间导致较为宽泛的解释和应用。	我们建议阐明本条下的数据安全审查将如何与网络安全法及个人信息保护法草案二次审议稿（"**个人信息保护法（草案二次审议稿）**"）所述的"安全评估程序"、数据安全风险评估（见第二十一条）、国信办颁布的

		指引草案以及各项行业标准相互联系。 我们建议如果金融机构已于上一年度执行安全评估程序，应豁免对其进行数据安全审查。 我们建议在数据处理活动的背景下澄清该等国家安全审查的性质。 已有若干现有和拟议的数据处理活动审查机制，如第三十条和网络安全法要求的跨境安全评估，并且为保护商业效率，不应创建任何重复性的流程。我们建议尽快发布明确规定审查触发的因素以及审查的范围和程序（包括法定办结时限）的实施细则。 应尽可能地考虑引入裁决上诉程序，至少应设置相关渠道以向相关方披露该等决策是如何做出的，从而为在作出决定时已考虑所有重要事实提供透明度。
24	We understand that the State will impose data export controls. We are particularly concerned about the following: (a) **What the data export controls entail** - for example, whether financial institutions will be subject to any obligations to disclose the details regarding the destination's network or cybersecurity, or to encrypt controlled items before transfer across border. (b) **Consequences of breach of data export controls** - for example, whether failure to comply with the data export controls would impact the ability to expand business in the PRC, or to obtain new licences.	We recommend clarifying if "controlled items" means "Controlled Items" as defined in the Export Control Law. If so, we submit that this requirement should be set out in the Export Control Law but not the DSL. If not, we recommend clarifying the scope of "controlled items". We also request expressly providing that the sharing, disclosure and transfer of data within the same corporate group (including between different branches) should not be subject to export controls regardless of whether the data is a "controlled item".
第二十四条	我们了解国家将实施数据出口管制。 我们尤为关注下列问题： 	我们建议阐明本条所述的"管制物项"是否是指《出口管制法》所界定的"管制物项"。如是，我们认为有关规定应在《出口管制法》而非数据

	(a) **数据出口管制的影响** – 例如，金融机构是否须履行任何披露与目的地网络或网络安全有关的详细资料的义务，以及是否须在进行跨境传输前加密管制物项。 (b) **违反数据出口管制的后果** – 例如，未能遵守数据出口管制是否影响其在中国发展业务或取得新业务经营许可的能力。	安全法内载列。如否，我们建议阐明“管制物项”的范围。 此外，我们请求明确规定，在同一公司集团内部（包括在不同分支机构之间）分享、披露和传输数据不会受到出口管制，不论有关数据是否为「管制物项」。
25	NA	We recommend clarifying: (a) what would amount to “discriminatory prohibitions, limitations or other such measures”; (b) that a private entity will not be affected even if it is incorporated in an impugned country; (c) the relevant authorities which will be responsible to supervise compliance of any measures adopted; and the specific circumstances and data types to which this Article 25 may apply.
第二十五条	不适用	我们建议阐明下列各项： (a) 什么情况属于「歧视性的禁止、限制或者其他类似措施」； (b) 即使私营实体在受质疑国家注册成立，亦不会受到影响； (c) 将负责监督遵守所采纳的任何措施的有关主管机构；及 本第二十五条可能适用的特定情况和数据类型。
Chapter IV Data Security Protection Obligations **第四章 数据安全保护义务**		
Chapter IV in general	Chapter IV of the DSL imposes a number of obligations on financial institutions.	We recommend detailed guidance to enable the financial institutions to understand their obligations and how to comply. Please also refer to our recommendations in paragraph 1 of **Part A**.

第四章整体	数据安全法第四章对金融机构施加一系列义务。	我们建议给予金融机构详细指引，让它明白其义务及如何遵行。亦请参阅甲部第 1 段。
26	We raise the following: (a) **Status of requirements** The reference to "administrative rules and regulations… and other measures" may have an unintended effect of requiring financial institutions and other private entities to adhere strictly to recommended standards which do not have the force of law in the first place. This article may expand the scope of application and uplift the punishment for existing requirements. We believe the original intention of those requirements should be upheld.	We recommend expressly clarifying that: • data activities should be conducted in compliance with mandatory requirements under the relevant laws and regulations; and • entities will not be required to adopt recommended standards or best practices (which should be in line with international standards as mentioned in our recommendation on Article 16), but they may do so voluntarily or choose other standards or practices that allow them to comply with the DSL, in light of their own circumstances and/or a particular fact pattern.
	我们的意见如下： (a) **有关规定的地位** 对"行政法规……及其他必要措施"的提述可能无意中要求金融机构及其他私营实体严格遵守建议的标准，而有关标准其实并无法律效力。 本条可能扩大现行规定的应用范围，增加处罚。我们认为应维持有关规定的原意。	我们建议明确说明： • 数据活动应遵守相关法律法规的强制性规定；及 • 至于建议标准或最佳惯例（如我们在有关第十六条的建议中所述，应与国际标准一致），实体不会被强制要求采纳，但它们可自愿采纳，或根据自身情况及/或特定实情选择遵守数据安全法允许的其他标准或惯例。
	(b) **Multi-level protection scheme** As noted in respect of Article 20, the Second Review DSL specifically mentions the MLPS on several occasions. However, many firms assert that there is a lack of detail in respect of practical compliance with the MLPS, including how to conduct assessments and grade systems in terms of the level of protection required, etc. This is	See our recommendations on Article 20 in respect of the potential for overlap and therefore confusion as a result of similar concepts being introduced in each of Articles 20 and 26. We suggest that regulatory supervision and enforcement in the area of MLPS must be balanced with the ability of financial institutions and other business to be able to comply

	particularly concerning to financial institutions due to the apparent increase in regulatory focus on ensuring MLPS compliance.	while the related rules and guidance are being formulated. Financial institutions would welcome the opportunity for more dialogue with industry regulators to improve, in particular, processes of self-assessment within industry guidelines. For efficient compliance with the MLPS regime, it will be crucial that financial institutions and other businesses have clear direction from the Commission and industry regulators that MLPS-related laws and regulations remain mandatory, but industry guidelines are only for reference.
	(b) **分类分级保护制度** 如我们在评论第二十条时所提到的，数据安全法（草案二次审议稿）有好几处特别提到了分类分级保护制度。 但有许多公司反映，草案对于如何在实践中遵守分类分级保护制度缺乏详细的规定，包括如何评估所需的保护程度以及如何对数据实行分类分级保护等。考虑到监管机构似乎越来越着力于确保对分类分级保护制度的遵守，这一点与金融机构的关系尤其密切。	请参见我们就第二十条指出的关于第二十条和第二十六条规定的近似概念有可能存在重叠和造成混淆提出的建议。 我们建议，监管机构在监督和执行分类分级保护制度时应取得平衡，使金融机构及其他企业在相关细则和指导意见出台之前能够确保合规运营。金融机构希望有机会与行业监管机构进行更多的沟通，特别是就如何改善行业指引框架内的自我评估程序这一点进行沟通。为了使金融机构及其他企业能够有效遵守分类分级保护制度，法工委和行业监管机构有必要清楚说明虽然与分类分级保护制度相关的法律和法规属于强制性质，但行业指引是仅供参考的。
	(c) **Responsible person and management body for data security** This article imposes direct obligations on financial institutions and other private entities to maintain responsible personnel and management body for the purpose of the data security protection.	To enable financial institutions to comply, we recommend expressly clarifying: • that the responsible person can share roles between group companies, affiliates or other similar data protection roles under other laws or regulations;

	However, no detailed guidance has been provided as to complying with these requirements.	• that the responsible person can have other roles; and • the obligations and potential liabilities of the responsible person and the management body or providing reference to other guidance such as in the Information security technology: personal information security specification (GB/T 35273-2020).
	(c) **数据安全的负责人和管理机构** 本条对金融机构及其他私营实体施加直接义务，要求私营实体就数据安全保护指定负责人及管理机构。 然而，本条并无就遵守该等规定提供详细指引。	为使金融机构遵守规定，我们建议明确规定： • 负责人可在集团公司或关联机构之间分担职责，或分担其他法律法规所规定的其他类似的数据保护职责； • 负责人可以有其他职责；及 负责人和管理机构的义务及潜在责任，或提示参考其他指导文件，例如《信息安全技术：个人信息安全规范》（GB/T 35273-2020）。
28	This article imposes a notification obligation on financial institutions in case of a data security incident.	The article requires notification to data subjects according to "regulations". We ask that the relevant regulations be sufficiently described to enable this Article 28 to be interpreted properly. We also suggest, as for the First Review DSL, clarifying to whom should a financial institution report in case of a data security incident. We also recommend detailed guidance on how the requirement will be applied and enforced. For instance, financial institutions may be subject to a duty of confidentiality to other parties (e.g. under contract). Such guidance should assist financial institutions to navigate those conflicting obligations.
第二十八条	本条规定金融机构在发生数据安全事件时须承担通知义务。	本条规定应按照"规定"通知资料当事人。我们请求对有关规定作详细描

		述，让本第二十八条得以适当解读。 正如我们对数据安全法（草案一次审议稿）提出的反馈意见，我们建议说明，如果发生数据安全事件，金融机构应向哪一方报告。 同时，我们建议就该规定的应用和执行制定详细指引。例如，金融机构可能须对他人遵守保密责任（如根据合同）。有关指引能够帮助金融机构建立有关程序，确保合规。
29	We refer to our comments on Article 20 with respect to the definition of "important data".	We suggest clarifying the triggering event for a financial institution to conduct data risk assessments and providing details of the assessment standards. We recommend that a financial institution should decide on the frequency of the data risk assessment having regard to the data security risks to which it is exposed. Please also refer to our recommendations on Article 21 above with regard to risk-based assessment.
第二十九条	谨此提述我们关于第二十条下对"重要数据"定义的意见。	我们建议说明金融机构进行数据风险评估的触发事件，并提供详细的评估标准。我们建议应由金融机构决定评估数据风险的频率，并在决定频率时考虑其所承受的数据安全风险。 另请参见我们在上文就第二十一条提出的关于风险导向评估的建议。
30	**(a) Data exports by critical information infrastructure ("CII")** We note the welcome clarification in Second Review DSL that security administration of outbound transfers of important data by operators of critical information infrastructure ("**CII**") is to be governed by the CSL. However, the security assessment regime under the CSL remains unexplained and the Second Review DSL does not provide further guidance in itself. In particular, neither the CSL nor Second Review DSL contain a definition of a CII operator.	**(a) Clarify scope of CII** We suggest clarifying the definition of "CII" operator under the DSL or expressly specifying that CII operator should have the same meaning as that under the CSL, and providing a definitive timetable for release and implementation of the 2017 Draft CII Measures or other measures which will set out an unambiguous term. We suggest the relevant sector regulators actively seek the views of market participants and involve them in the process of formulating the

	Although a partial definition was provided under the CSL and a two-limb test to determine whether IT networks constituted CII was proposed under the draft Measures on Security Protection of Critical Information Infrastructure issued in July 2017 ("**2017 Draft CII Measures**"), these draft rules were never enacted. As such, financial institutions cannot be sure whether same definition should apply under the DSL and, if so, when the relevant provisions of the draft rules will be settled. **(b) Expansion of localisation requirements** Despite the clarification above, uncertainty for financial institutions and other business is increased by the suggestion that cross-border transfers of data by other organisations and individuals may be regulated further in rules to be formulated by the CAC and other competent departments of the State Council. Therefore, the lack of additional information on the meaning of "important data" and a timetable for any other measures to be released is unwelcomed uncertainty for businesses operating on a cross-border basis, particularly given the breadth of proposed restrictions introduced in draft measures and guidelines previously.	definition of "CII" and any accompanying requirements for a particular sector. Please also refer to our recommendations on having the PBOC as the lead and co-ordinating regulator for financial institutions in respect of Article 6. **(b) Minimise localisation requirements** We strongly assert that any additional proposals around data localisation should be reconsidered, as localisation of data does not serve effectively to improve protection of interests unless the scope of restrictions to be administered effectively by business and government is very well defined and as narrow as not to unduly stifle legitimate business. If that is not the case, localisation requirements give rise to many disadvantages including curtailing the financial industry's growth and compromising the effectiveness of cybersecurity, risk management controls and business continuity, with restrictions serving to reduce product and service offerings, and impair the quality of any offerings, to Chinese customers, and ultimately negatively impact the PRC's role and participation in international trade flows. However, if the Commission believes the possibility of imposing additional localisation requirements must be retained, we would strongly suggest that a definitive timetable for release and implementation of the relevant rules is provided at or before the finalisation of the DSL. Please also see our comments on Article 24.
第三十条	**(a) 关键信息基础设施进行的信息出境** 我们注意到，数据安全法（草案二次审议稿）对关键信息基础设施运营者	**(a) 明确关键信息基础设施的范围** 我们建议明确数据安全法下的关键信息基础设施运营者的定义或者明确规

	的重要数据出境安全管理作出了澄清，即应适用网络安全法，这一结果受到普遍欢迎。但是，网络安全法下的安全评估制度仍有待解释，而数据安全法（草案二次审议稿）本身并未给出进一步的指导。特别是，网络安全法和数据安全法（草案二次审议稿）均未对关键信息基础设施的运营者作出定义。尽管网络安全法作出了部分定义，且2017年7月发布的《关键信息基础设施安全保护条例》草案（"**2017 关键信息基础设施条例草案**"）提出采用两项标准测试来判断信息技术网络是否构成关键信息基础设施，但上述规则草案并未正式制定。因此，金融机构无法确信数据安全法也适用同一定义以及若适用该定义，规则草案中的相关规定将何时正式施行。 **(b) 扩大本地化要求** 尽管作出了上述澄清，金融机构和其他企业所面临的不确定性却在增加，因为有迹象表明，其他组织和个人的跨境数据转移可能受到国信办和国务院下属其他主管部门所制定规则的进一步规范。因此，"重要数据"的含义缺乏补充资料以及任何其他待发布条例缺乏时间表都是跨境运营企业不希望面对的不确定因素，特别是考虑到此前条例草案中拟议引入的限制性规定范围都较广。	定，关键信息基础设施运营者应具有网络安全法所规定的含义，并给出2017 关键信息基础设施条例草案或其他明确该等定义的其他条例确切的颁布和实施时间表。 我们建议有关行业监管者积极征求市场参与者的意见，邀请其参与关键信息基础设施定义以及特定行业的任何相关要求的制定流程。同时请参阅我们就第六条提出的指定央行作为金融机构的牵头协调监管机构的建议。 **(b) 最大限度降低本地化要求** 我们强烈建议任何关于施加额外本地化要求的规定应该被重新考虑，因为除非非常明确地界定企业和政府实际管理的限制范围并尽可能缩窄范围以避免不合理地抑制商业发展，否则数据本地化难以有效促进权益保护，而且会产生诸多弊端，包括阻碍金融业发展以及有损网络安全、风险管理控制和商业持续性。该等限制性规定将降低向中国消费者提供的产品和服务的数量与质量，最终对中国在国际贸易中的作用和参与度产生负面影响。 不过，如果法工委认为应保留施加额外本地化要求的规定，我们强烈建议在数据安全法定稿的同时或定稿之前提供相关规则明确的颁布和实施时间表。 同时请参阅我们关于第二十四条的意见。
31	NA	We recommend amending Article 31 as follows: *"Any organization or individual collecting data must adopt lawful and proper methods; they may not steal data or obtain it by other illegal means. Where laws and administrative regulations contain provisions on ~~the purpose or scope of data~~ collection or use, or both, of data, data shall be collected for a lawful purpose and used in accordance with the purpose(s) for which the ~~purpose~~*

		~~and within~~ data was collected. An organization or individual shall collect only such data as is needed for the ~~scope prescribed by laws and administrative regulations~~ intended purpose." We also recommend clarifying the ambit of "data collection" in this article.
第三十一条	不适用	我们建议对第三十一条作出如下修订： "任何组织、个人收集数据，必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用（或收集和使用）数据~~的目的、范围~~有规定的，应当在~~法律、行政法规规定~~合法的目的~~和范围~~内收集数据~~、~~，并根据收集数据的目的使用数据~~，不得超过必要的限度~~。任何组织、个人只可在预期目的所需的范围内收集数据。" 同时，我们建议明确本条内"数据收集"的范围。
32	We welcome the Government's positive attitude towards data transaction activities. We submit that the current regulatory requirements on data protection in the financial sector are stringent and data activities conducted by financial institutions are subject to strict regulatory oversight and involve intricacies of various existing laws and regulations, including those relating to anti-money laundering and counter-terrorism financing. It is extremely costly and complicated for financial institutions to revise their existing practices to address any changes in legal or regulatory requirements. The interplay of the new and existing requirements may also create unintended consequences for data subjects.	We suggest caution in imposing any new regulatory requirements on data transaction activities. We also suggest the Commission to consult the relevant authorities, and industry stakeholders to ensure that they are practicable and workable. As was the case for the First Review DSL, financial institutions will require further details on data transactions (eg what types of data may be transacted, the extent to which the data may be further transacted, how issues such as breach of confidentiality or secrecy should be dealt with) to provide meaningful comments regarding to any potential data transaction with respect to financial data. If the Commission intends to allow data transactions with respect to financial information, the Commission should work together with PBOC to

		ensure existing rules are updated to reflect this policy. Please also refer to our recommendation is paragraph 1 of **Part A**.
第三十二条	我们欢迎政府对数据交易活动持正面态度。 我们认为金融行业的现行数据保护监管规定十分严谨，金融机构开展数据活动受到严格的监管，并涉及不同现行法律法规之间的复杂关系，包括与反洗钱和打击恐怖分子资金筹集有关的法律法规。 金融机构修改其现有惯例以符合法律或监管规定的变动将牵涉高额成本和繁杂工作。新规定与现行规定之间的相互影响也可能对数据主体带来难以预料的后果。	我们建议为数据交易活动订立新监管规定时需要谨慎行事。我们也建议法工委咨询有关主管机构和业内持份者的意见，确保有关规定切实可行、行之有效。 与数据安全法（草案一次审议稿）相同，金融机构需要有关数据交易的进一步详细资料（例如可以进行交易的数据类型、数据可进一步交易的程度、如何处理违反保密或机密原则的问题等），以就有关金融数据的潜在数据交易提供实质意见。 如果法工委有意允许金融务数据交易，法工委应与央行合作，确保现行规则已更新以反映该政策。请亦参阅我们在甲部第 1 段的意见。
33	NA	We make the following recommendations here: (a) **Scope of the licensing regime for "data processing related services"** We recommend defining "data processing related services" to clarify the scope of the licensing regime. We further submit that foreign entities should also be eligible to apply for licences to operate "data processing related services". (b) **How the new licensing regime interacts with existing law** We recommend clarity as to how this new licensing regime will interact with the administrative licensing requirements for telecommunication business under the Telecommunications Regulations.

第三十三条	不适用	我们的建议如下： **(a) “数据处理相关服务”的经营许可颁发制度范围** 我们建议界定“数据处理相关服务”，以厘清经营许可颁发制度的范围。 我们进一步建议，境外实体应合资格申请“数据处理相关服务”经营许可。 **(b) 新的经营许可颁发制度与现行法例的关系和相互作用** 我们建议厘清新的经营许可颁发制度与《电信条例》下颁发电信业务经营许可的行政规定如何相互作用。
34	As for the First Review DSL, we submit that this article does not provide sufficient details relating to the scope of investigation or enforcement powers, who may exercise such powers, and how they may be exercised. This is particularly the case for international financial institutions. Such further details are essential to enable those financial institutions to formulate and implement appropriate internal measures (e.g. privileged access, authentication activities, user credentials, mail attachments and uploading/downloading activities) to monitor and manage data security and to ensure compliance with the DSL. We reiterate our comments and recommendations on Article 2 in this **Part B** that the investigatory power by the relevant public security departments and national security departments should not cover non-PRC Data Activities. See also our comments on the DSL's extraterritoriality in paragraph 3.1 of **Part A**.	We recommend providing specific details regarding the following items as was the case for the First Review DSL: (a) the relevant laws and regulations referred to in Article 34 with which the public security departments and national security departments are required to comply; (b) the contact details of each relevant public security department and national security department in respect of any investigation or enforcement of the DSL; (c) how data may be collected by the relevant public security departments or national security departments, and how they will make such requests for data, including details on: • how they may exercise their powers to request data stored outside the PRC for the purpose of investigating any Harmful Non-PRC Data Activities; and • the approval procedures that they need to go through to the

		request data for the purpose of investigations.
第三十四条	与数据安全法（草案一次审议稿）相同，我们认为，本条对侦查范围、执法范围、执法人员和执法方式的细节描述不充分。 对国际金融机构来说更是如此。 在本条提供更多详情十分重要，这有助金融机构制定和实施适当的内部措施（如存取特权、认证活动、客户凭证、邮件附件和上传／下载活动等），以监控和管理数据安全，确保遵守数据安全法。 我们重申在乙部作出的有关第二条的意见和建议，我们认为有关公安机关和国家安全机关的侦查权力不应覆盖中国境外的数据活动。同时请参阅甲部第 3.1 段我们有关数据安全法域外法权的意见。	与数据安全法（草案一次审议稿）相同，我们建议就下列各项补充具体说明： (a) 第三十四条所述，公安机关和国家安全机关须遵守的有关法律法规； (b) 与数据安全法相关侦查和执法有关的各相关公安机关和国家安全机关的联络资料； (c) 有关公安机关或国家安全机关收集数据和要求提供数据的方式，包括有关下列各项的详情： • 该等机关会如何行使权力要求提供存储于中国境外的数据，以用作侦查有害的中国境外数据活动；及 • 该等机关要求提供数据进行侦查时须遵守的审批手续。
35	We refer to Article 177 of the Securities Law and the draft Article 136 of the Futures Law which restricts the disclosure of securities business-related data to overseas regulators. We understand that the existing position is now proposed to be expanded to cover any and all data stored within the PRC that may be requested by foreign judicial and law enforcement bodies, similar to the obligation in respect of personal information under Article 41 of the Second Review PIPL. In addition, we note in the Second Review DSL that the ability to provide data in accordance with international mutual assistance treaties and similar agreements to which the PRC is a party no longer prevails over the DSL restrictions. We continue to submit that this expansion will create major issues for global financial institutions	As in our submission for the First Review DSL, we strongly recommend expressly clarifying that this article does not apply: (a) to the types of data that are not likely to endanger national security or public interest. These types of data should be expressly set out in the DSL or any related rules or regulations; (b) to data stored in the PRC merely by virtue of its storage in a cloud server located in the PRC; (c) if there is no data export (ie if a copy of the data is already lawfully stored outside the PRC offshore before a foreign judicial or law enforcement body makes a request for the data in the jurisdiction where it is stored outside PRC); (d) when the data export is to facilitate intra-group assessment

	headquartered outside of the PRC, as it is likely to conflict with existing legal requirements under the laws of other jurisdictions. For example: • financial institutions may be required by the foreign regulator to respond within a time limit; and • if PRC authorities refuse to provide an approval to disclose, then the financial institutions may be in breach of the law of the other jurisdiction.	or reporting for anti-money laundering and counter-terrorism financing purposes; or (e) to provision of data to international organisations (e.g Interpol), re-instating the exception from the First Review DSL allowing organisations to observe international mutual assistance treaties and similar agreements to which the PRC is a party. We also ask that the meaning of "foreign law enforcement bodies" be clarified: in particular, whether financial regulators, tax bureaus, exchanges and clearing houses will be considered "foreign law enforcement bodies". We recommend that relevant authorities also expressly revise similar existing restrictions (eg. CSRC's restriction on the sharing of "any securities business related data" without CSRC approval, and CBIRC's restriction on the transmission of client data to an offshore vendor regardless of whether the data is encrypted). See also our recommendations on Article 11.
第三十五条	据我们所知，《证券法》第一百七十七条及《期货法（草案）》第 136 条限制向境外监管机构提供与证券业务活动有关的数据。 我们了解到，与个人信息保护法（草案二次审议稿）第四十一条项下个人信息的相关义务类似，目前的情况是建议将有关范围扩大至涵盖境外司法和执法机构要求提供的在中国存储的一切数据。 此外，我们注意到在数据安全法（草案二次审议稿）中，根据中国缔结或者参加的国际条约和协议提供数据的	正如我们对数据安全法（草案一次审议稿）提出的反馈意见，我们强烈建议明确说明本条不适用于下列情况： (a) 不太可能危害国家安全或公共利益的数据类型。数据安全法或任何相关规则或法规应明确列明有关数据类型； (b) 纯粹通过使用位于中国境内的云服务器存储于中国境内的数据； (c) 并无数据出口情况（即在境外司法或执法机构要求提供数据前，已在有关中国境外的司法管辖区

	权利已不再优先于数据安全法所规定的限制。 我们仍然认为，扩大有关范围很可能会与其他司法管辖区法律下的现行法律规定冲突，对总部位于中国境外的国际金融机构造成重大困扰。例如： • 境外监管机构可能要求金融机构在一定时间内作出回应；及 • 如果中国主管机构拒绝批准资料披露，有关金融机构可能会违反其他司法管辖区的法律。	合法存储该等数据的离岸副本）； (d) 数据出口旨在协助进行集团内部的反洗钱和打击恐怖分子资金筹集评估或报告；或 (e) 向国际组织（如国际刑警组织）提供数据，重新采纳数据安全法（草案一次审议稿）中允许各组织遵守中国缔结或者参加的国际条约、协定的优先适用的表述。 同时，我们请求阐明“境外执法机构”的涵义：尤其是，金融监管机构、税务局、交易所和结算所是否属于“境外执法机构”。 我们建议，相关主管机构同步修改现行的类似限制（例如，证监会禁止在未经其批准的情况下分享“与证券业务活动有关的数据”、中国银保监会限制向离岸供应商传送客户资料（不论是否已加密））。 同时请参阅我们有关第十一条的建议。
Chapter V Government Data Security and Openness **第五章 政务数据安全与开放**		
39	This article appears to suggest that State organs must monitor the performance of data security obligations by all parties that receive “government affairs data”.	We recommend clarifying the scope of “government affairs data” as financial institutions that are recipients of such data will otherwise not have a clear idea that they are recipients of it and therefore that they have corresponding obligations.
第三十九条	本条似乎暗示国家机关必须监督“政务数据”的所有收取方对数据安全义务的履行。	我们建议明确“政务数据”的范围，否则收取这些数据的金融机构无法清楚地判断自身是否是政务数据收取方并因而需要承担相应的义务。
41	We welcome the opening up of public data for use by firms which may drive data innovation and the use of data for public good and societal benefits. This is essential to facilitate green finance and sustainability.	In this regard, we recommend defining “government data” and providing more details on how the opening up of government data may be balanced against the confidentiality of information provided

	However, we are concerned that financial institutions may lose their rights over data provided to government authorities, including any such data that may be aggregated or combined with government data.	to government authorities by the firms regulated by them.
第四十一条	我们欢迎开放公共数据予公司使用，以推动数据创新和使用数据为公众和社会谋求利益。数据开放对促进绿色金融和可持续发展有着关键作用。 可是，我们关心金融机构可能会失去其对提供给政府部门的数据（包括与政务数据汇总或合并的任何该等数据）享有的权利。	就此而言，我们建议界定“政务数据”的涵义，并具体说明如何在政务数据开放与受政府部门监管的公司向政府部门提供的信息的保密性这两者之间取得平衡。
Chapter VI Legal Liability **第六章 法律责任**		
Chapter VI in general	NA	Please clarify which competent authority (or authorities) will enforce the DSL with respect to financial institutions.
第六章整体	不适用	请列明对金融机构执行数据安全法的主管机构。
43	NA	Please clarify the criteria in finding a “material security risk in data activity”.
第四十三条	不适用	请列明发现“数据处理活动存在较大安全风险”的标准。
44	(a) **Lack of clarification on the trigger for sanctions** While we appreciate the Government’s desire to raise the importance of data security compliance through meaningful sanctions for failure to comply and, indeed, the increase in the level of fines proposed in the Second Review DSL compared to the First Review DSL, we would like to point out that the mechanism for triggering liability and the quantum of any such liability must be completely transparent and unambiguous.	**(a) Clarify trigger for serious violations** We recommend clarifying what amounts to a serious violation. Avoiding non-compliance is, of course, all financial institutions’ objective, but it is an important principle of the rule of law to understand the penalties that could be applied on a breach. **(b) Clarify responsible persons** We suggest clarifying the definitions of “directly liable persons in charge”

	(b) **Lack of clarification on the "directly liable persons in charge" and "other directly responsible personnel"** The "directly liable persons in charge" and "other directly responsible personnel" may be subject to fines under certain circumstances while there is no definition of these two terms. In particular, it is unclear whether the legal representative would be held responsible if he/she is not involved in data processing activities. Given the magnitude of personal liability involved, it is crucial for senior management of financial services firms to understand the scope of these terms.	and "other directly responsible personnel". We also recommend that the threshold for individual liability be clarified and set sufficiently high (e.g. fraud and intentional breach rather than only negligence) to ensure that individuals understand their risk exposure but are not unnecessarily deterred from participating in these roles.
第四十四条	**(a) 没有对处罚的触发标准作出清晰界定** 虽然我们理解政府希望通过对违法行为给予实质性处罚来强化数据安全合规的重要性以及《数据安全法》（二次审议稿）建议的罚款金额确实比《数据安全法》（一次审议稿）有所增加，但我们想指出，相关法律责任的触发机制以及每一法律责任对应的具体数额应当完全透明且不含糊。 **(b) 没有对"直接负责的主管人员"和"其他直接责任人员"作出清晰界定** 在某些情形下，"直接负责的主管人员"和"其他直接责任人员"可被处以罚款，但对这两个术语却没有给出定义。尤其是对于法定代表人在其未参与数据处理的情形下是否须负责这一点没有予以明确。鉴于所涉及的个人责任金额较大，让金融服务企业的高级管理人员理解相关术语的涵盖范围是非常重要的。	**(a) 明确严重违法的界定标准** 我们建议对何为情节严重作出清晰规定。当然，避免违法行为是所有金融机构的目标，但了解对违法行为可能进行的处罚亦尤为重要。 **(b) 清晰界定责任人** 我们建议，对"直接负责的主管人员"和"其他直接责任人员"作出清晰界定。 我们还建议明确触发个人法律责任的门槛，并将门槛设置在一个充分高的水平（例如，欺诈和故意违法而非仅为过失），以确保相关个人均能明白其风险敞口，但又不会对其担任相关职务造成不必要的妨碍。
46	We note that the Second Review DSL includes additional penalties in	We recommend that this article (or Article 34) is elaborated to clarify that

	instances where organisations or individuals do not cooperate with public and national security authorities in providing access to data. However, as stated in our comments on Article 34, the Second Review DSL does not provide sufficient details relating to the scope of investigation or enforcement powers, who may exercise such powers, and how they may be exercised. As such, it is difficult, if not, impossible for financial institutions or their personnel to comply with these requirements and therefore there may be a real risk of violation of these rules through no objective fault of the organisation and/or individual in question.	any sanctions applicable in this regard will only be triggered where there has been no attempt on the part of financial institutions or their personnel to comply, and that the Commission or competent authorities seek to provide further guidance on the requirements and process under Article 34 as soon as possible.
第四十六条	我们注意到，《数据安全法》（二次审议稿）包括了组织或个人在提供数据访问方面不配合公共和国家安全机关的情况下的额外处罚措施。但正如我们在对第三十四条的建议中所述，《数据安全法》（二次审议稿）并没有提供关于调查或执法权的范围、谁可以行使这些权力以及如何行使这些权力的更多细节从而，由于金融机构及其工作人员很难遵守这些规定，因此，可能存在相关组织和/或个人在没有客观过错的情况下却违反这些规定的实际风险。	我们建议对本条（或第三十四条）进行详细阐述，以明确只有在金融机构或其人员并未试图遵守这些规定时才会触发这方面的相关处罚，同时建议法工委或主管部门尽快就第三十四条项下的要求和程序提供进一步的指导。
48	We submit that private entities should be entitled to civil compensation with respect to any infringement of their rights to trade secrets or proprietary information caused by a government employee's negligence or abuse of power.	We recommend amending the Article as follows: *"If government employees with the responsibility of overseeing data security neglect their duty, abuse their power, infringe trade secrets or other proprietary information, or abuse their position for private gain, yet it does not constitute a crime, they shall be sanctioned in accordance with the law and liable for civil compensation for*

		infringements of trade secrets and proprietary information.” Please clarify that “government employees” referred to in this article means any persons employed by the (PRC) Government who are responsible for supervising any and all data activities with respect to data security.
第四十八条	我们认为，如果国家工作人员玩忽职守、滥用职权而造成任何侵犯私营实体的商业机密或专有信息权利的行为，该私营实体有权获得民事赔偿。	我们建议对本条作下列修改： *“履行数据安全监管责任的国家工作人员玩忽职守、滥用职权、侵犯商业机密或其他专有信息、徇私舞弊，尚不构成犯罪的，依法给予处分，并就其侵犯商业机密和专有信息的行为作出民事赔偿。”* 请说明本条所述“国家工作人员”是指任何受雇于（中国）政府，负责监管数据活动保障数据安全的人士。
53	We note that no timetable is stated in the Second Review DSL for the effectiveness of the DSL.	We suggest that the period should be at least 24 months from finalising the form of the DSL. If, for any reason, relevant sectoral rules cannot take effect at the same time as the DSL, we suggest an implementation period of 24 months after the sectoral rules are finalised, to enable financial institutions to fully understand the implications and formulate and implement the necessary compliance measures.
第五十三条	我们注意到，《数据安全法》（二次审议稿）并没有说明《数据安全法》的生效日期。	我们建议，生效日期应在数据安全法最终版本确定时起至少满 24 个月以后。如果因任何原因，相关行业规则无法与数据安全法同时生效，我们建议，相关行业规则最终确定后应有一个 24 个月的过渡期，以使得金融机构能够完全了解相关影响并制定和实施必要的合规措施。