16 August 2020
2020 年 8 月 16 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 Data Security Law
《数据安全法》征求意见稿

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] and the Futures Industry Association ("**FIA**")[2] (together, the "**Associations**" or "**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 Data Security Law ("**DSL**") of the People's Republic of China ("**PRC**") published on the National People's Congress website[3].

亚洲证券业与金融市场协会（「**ASIFMA**」）[1] 和「**FIA**」[2]（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》征求意见稿[3]（「**数据安全法**」）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。

---

1 ASIFMA is an independent, regional trade association with more than 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Through the GFMA alliance with SIFMA in the US 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 100 多家来自买方和卖方市场的领先机构组成。ASIFMA 通过全球金融市场协会（GFMA）与美国的证券业与金融市场协会（SIFMA）及欧洲的金融市场协会（AFME）形成联盟，共同提供全球最佳行业实践及标准，为区域发展作贡献。

2 FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in London, Singapore and Washington, D.C. FIA's membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from more than 48 countries as well as technology vendors, lawyers and other professionals serving the industry. FIA's mission is to support open, transparent and competitive markets, protect and enhance the integrity of the financial system, and promote high standards of professional conduct. As the principal members of derivatives clearinghouses worldwide, FIA's member firms play a critical role in the reduction of systemic risk in global financial markets. Further information is available at www.fia.org

FIA 是国际领先的期货、期权和中央结算衍生工具市场贸易组织，分别在伦敦、新加坡和华盛顿设有办事处。FIA 会员基础广泛，包括遍布 48 余个国家的结算公司、交易所、结算所、交易公司、商品专业人士，以及服务业界的技术供应商、律师事务所和其他专业机构。FIA 致力创造公开、透明和具竞争力的市场，保护并健全金融体系，促进高标准的专业操守。FIA 的成员公司包括全球衍生工具结算所的主要成员，在减少全球金融市场系统风险方面发挥着重要作用。更多资料请查阅：www.fia.org

3 Available at: http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808172b5fee801731385d3e429dd.
可于以下网址查阅：http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808172b5fee801731385d3e429dd。

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

FIA - Level 18, Centennial Tower
3 Temasek Avenue
Singapore 039190
Tel: +65 6950 0691

We have consulted our members and received responses. This letter sets out our views on the DSL, the practical difficulties financial institutions may face and our recommendations and our request for clarification for certain provisions of the DSL.

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对数据安全法若干条文明晰化的请求。

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 DSL casts a broad net, 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 – and indeed, the future Personal Information Protection Law - is also unclear.

同时，数据安全法涵盖范围广泛，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的要求和期望，以及将有《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**。

At a high level, our key concerns are as follows:

我们最为关心的主要问题如下：

(a) **Overarching concerns**
整体考虑

The DSL will inevitability impact the business operations of financial institutions in many ways. However, the DSL as currently drafted is broadly worded and lacks specific guidance in key areas of concerns. These give rise to uncertainties in the mind of financial institutions, particularly, regarding the following aspects:

(i) Broad scope of application of the DSL and its extraterritorial application.

(ii) Overlap with existing laws and regulations. In particular, data activities conducted by financial institutions are highly regulated, so it is critically important that areas of duplication or inconsistency are resolved before implementation.

(iii) Principle-based obligations which will require more specific guidance to enable compliance in practice.

数据安全法将不可避免地会在许多方面对金融机构的业务经营造成影响。然而，目前数据安全法草案措词宽泛，缺少对有关问题在关键领域的具体指引。这导致金融机构存有疑虑，尤其是在下列几个方面：

(i) 数据安全法的广泛应用范围及其域外适用问题。

(ii) 与现行法律法规重叠。尤其是，金融机构开展的数据活动受到高度监管，因此，在数据安全法实施前厘清法律重叠的范围或分歧，十分关键。

(iii) 原则性义务的实际遵守需要更具体的指引。

Further details are set out in **Part A** of the Appendix.

进一步详情载于附件**甲部**。

(b) **Specific items**
具体问题

Certain Articles impose direct obligations and risks on financial institutions, and they generally invoke more concern amongst our members. They include:

(i) the broad definitions of "data", "data activities" and "data security" in Article 3;

(ii) the impact on existing data regulatory landscape caused by Articles 6 and 7;

(iii) the promotion of cross-border data transfer referred to in Article 10;

(iv) the tiered data security system and the classification of data as "important data" set out in Article 19;

(v) the framework to be set up for security impact assessment, reporting, sharing, monitoring, inspection/ review systems in Articles 20 and 22; and

(vi) data security protection obligations imposed on financial institutions under Chapter IV.

若干条款令金融机构须承担直接义务和风险，引起协会会员较深切的关注，包括：

(i) 第三条有关「数据」、「数据活动」和「数据安全」的定义宽泛；

(ii) 第六、七条对现有数据监管架构的影响；

(iii) 第十条所述关于促进数据跨境流动；

(iv) 第十九条所载关于数据安全分级制度以及「重要数据」的分类标准；

(v) 第二十、二十二条所述关于建立安全风险评估、报告、共享、监测、检查/审查制度的机制；及

(vi) 第四章对金融机构施加的数据安全保护义务。

We set out our specific comments and provide our recommendation with respect to each Article in **Part B** of the appendix.

我们有关上述条款的具体意见和建议载于附件**乙部**。

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 do not hesitate to contact Matthew Chan, ASIFMA Head of Policy and Regulatory Affairs, at mchan@asifma.org or +852 2531 6560, and TzeMin Yeo, FIA Head of Legal & Policy, Asia Pacific, at tmyeo@fia.org or +65 9111 0717.

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）和 FIA 亚太法律和政策事务总监 TzeMin Yeo（电邮：tmyeo@fia.org，电话：+65 9111 0717）。

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 King & Wood Mallesons, based on feedback from the wider ASIFMA and FIA membership.

本函件在金杜律师事务所的协助下，根据 ASIFMA 和 FIA 会员的广泛反馈意见撰写。

Yours faithfully
顺颂商祺

Mark Austen
Chief Executive Officer
Asia Securities Industry & Financial Markets Association (ASIFMA)

Bill Herder
Head of Asia-Pacific
Futures Industry Association (FIA)

Appendix – Detailed comments
附件 – 具体意见

Introduction
绪言

This Appendix is structured as follows:

本附件由以下部分构成:

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 DSL, and any reference to the "**DSL**" is a reference to the draft DSL published on the National People's Congress website as at the date of this submission.

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解释。「**数据安全法**」指截至本函件日期在中国人大网所登载的数据安全法草案。

Part A Overarching comments
甲部 整体意见

1 **Scope of application**
应用范围

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:

(a) jurisdictional reach (see paragraph 1.1); and

(b) the definition of key concepts (see paragraph 1.2).

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) 司法管辖范围（详见第 1.1 段）；及

(b) 主要概念的定义（详见第 1.2 段）。

1.1 Extraterritoriality
域外法权

The DSL covers:

(a) data activities conducted within the PRC[4] ("**PRC Data Activities**"); and

(b) data 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**").

数据安全法涵盖：

(a) 在中国[4]境内开展的数据活动（「**中国数据活动**」）；及

(b) 中国境外的组织、个人开展的，损害中国国家安全或者中国公民、组织的合法权益的数据活动（「**有害的中国境外数据活动**」）。

We understand that the DSL is intended to apply to all PRC Data Activities, and Harmful Non-PRC Data Activities will be subject to legal liability in accordance with the law (generally).

我们了解到，数据安全法拟适用于一切中国数据活动，并对有害的中国境外数据活动依法追究法律责任。

We strongly urge that the DSL focus on PRC Data Activities. The provisions in the DSL, whereby any data 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 conflict legal obligations for businesses, which are of serious concern to the 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。根据数据安全法的条文，在中国境外开展的任何数据活动，如果损害中国国家安全或公民、组织合法权益，就会触发第二条的法律责任，此规定过于宽泛，可以有多种解读，导致业务的各项法律义务相互冲突，因此业界极为关注。

[4] In this response, we refer to "PRC" as the People's Republic of China, excluding the Hong Kong and Macau Special Administrative Regions, and Taiwan, which we understand is consistent with the intent of the DSL.
在本文件中，「中国」指中华人民共和国，不包括香港特别行政区、澳门特别行政区和台湾，与我们所理解的数据安全法的定义一致。

Having regard to the strategic importance of data, its need and ability to move cross-border, 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。

Our two key areas of concern are as follows.

我们关注的两个主要领域如下。

Breadth and potential misalignment of jurisdiction
司法管辖权的范围和潜在偏差

First, we believe that the DSL is too broad and uncertain in its extra-territorial reach. 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 already particularly onerous given there may be very limited PRC nexus at all, with data potentially collected and stored wholly outside of the PRC.

首先，我们认为数据安全法涵盖范围过于广泛，且其域外应用范围存在不确定性。具体而言，如果中国境外的个人和组织无法以明确客观参数合理地作出评估，那么中国境外的个人和组织将难以应用数据安全法于其开展的活动。根据草案，域外应用范围非常广泛，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。

Furthermore, as noted above, the DSL's jurisdictional reach also exceeds that of the Cybersecurity Law. We submit that the extra-territorial application of the existing Cybersecurity Law is sufficient to safeguard national security. The very fact of the difference in jurisdictional reach of the DSL and the Cybersecurity Law creates a degree of complexity that has already caused serious concerns amongst foreign financial institutions. We believe restricting the DSL's extra-territorial application to a smaller scope or one that is commensurate with the Cybersecurity Law, 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. See also our comments in paragraph 2.

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若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。详见我们在第 2 段提出的意见。

Finally, where certain provisions are *not* intended to apply to data 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，如果无意对中国境外开展的数据活动应用部分条文，则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保护法第四章所载列的所有数据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。

Investigation and enforcement powers
调查和执法权

We are also particularly concerned about the scope of investigation and enforcement powers of the relevant PRC authorities over foreign entities, and we recommend more clarity in this regard.

我们还特别关心有关中国主管机构对境外实体进行调查和执法的范围，我们建议可以就此作出更明确的规定。

We welcome clarity on how the DSL will be enforced in practice, in terms of:

(a) communicating standards and expectations;

(b) undertaking investigations; and

(c) levying penalties.

我们欢迎对数据保护法在下列方面的实际执法方式作出明确说明：

(a) 沟通标准和预期；

(b) 展开调查；及

(c) 征收罚款。

Additional specific comments
其他具体意见

We provide specific comments on Article 2 of the DSL in **Part B**.

我们有关数据安全法第二条的具体意见载于**乙部**。

1.2 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 activities", which, respectively, read as follows:

> *"Data" refers to any record of information in electronic or non-electronic form.*

"Data activities" refers to data collection, storage, processing, use, provision, transaction, publication, and other such activities.

数据安全法的应用范围取决于「数据」和「数据活动」的定义，根据数据安全法：

「数据」是指任何以电子或非电子形式对信息的记录。

「数据活动」是指数据的收集、存储、加工、使用、提供、交易、公开等行为。

These definitions are very broad. 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.

上述定义范围非常宽泛。我们建议数据安全法对有关定义作出更具体的说明，将规管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。

We also strongly believe that inclusive definitions and terms like "other such activities" should be avoided, as they are very difficult to apply in practice and carry a high risk of inconsistent application.

同时，我们强烈认为，「其他类似活动」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。

Additional specific comments
其他具体意见

We provide specific comments on Article 3 of the DSL in **Part B**.

我们有关数据安全法第三条的具体意见载于**乙部**。

2 Overlap with other laws
与其他法律重叠

The wide scope of application of the DSL causes overlap with existing laws, regulations and guidelines.

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。

For example, the Cybersecurity Law 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 amongst the DSL, the existing Cybersecurity Law 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. Similar issues may also arise with respect to the existing Archives Law.

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，在现行档案法方面亦存在类似问题。

We seek clarification and detailed guidance on how the DSL will interact with these laws. We also provide specific comments on Article 49 of the DSL in **Part B** with respect to its relation with the Law on Guarding State Secrets.

因此，我们希望能够阐明数据安全法将如何与该等法律相互作用，并就此作出详细指引。我们有关数据安全法第四十九条与《保守国家秘密法》之间的联系的详细意见载于**乙部**。

In addition to reducing overlap and ensuring compatibility with *existing* laws, we suggest also factoring in laws that are in the pipeline, such as:

(a) the **Civil Code of the PRC** which was adopted by the 13th NPC and will take effect on 1 January 2021 contains provisions relating to personal data protection and privacy; and

(b) the **Personal Information Protection Law**, which is being drafted by the Commission, as announced on the NPC website on 15 May 2020.

We recommend refining the scope to minimise any overlap with these and other data-related laws.

除减少与*现行*法律的重叠部分，确保与现行法律相容以外，我们还建议把将予施行的法律纳入考量，如：

(a) **中国民法典**，已于第 13 届全国人大通过，并将于 2021 年 1 月 1 日起施行，当中载有与个人信息保护和隐私权有关的规定；及

(b) **个人信息保护法**，根据中国人大网 2020 年 5 月 15 日的公告，正在由法工委起草。

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。

Furthermore, we suggest specifying (or providing ancillary guidance as to):

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

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

此外，我们建议具体说明下列各项（或提供辅助指引）：

(a) 如果有与其他法律、法规或指引不一致的情况，将会怎么处理；及

(b) 数据安全法如何与其他法律、法规或指引相互作用。

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 harmonise the DSL with the other laws, regulations and guidelines. For example, other than the Cyberspace Administration of China ("**CAC**"), the People's Bank of China ("**PBOC**") and the China Securities Regulatory Commission ("**CSRC**") have also previously issued regulatory requirements relating to data security and data protection.

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。例如，除国家互联网信息办公室（「**国信办**」）外，中国人民银行（「**央行**」）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。

Additional comments
其他意见

See a specific example of how the DSL may overlap in our comments on Article 3 of the DSL in **Part B**.

乙部载有我们就数据安全法第三条作出的意见，当中会列举有关数据安全法可能会如何与现行法律法规重叠的具体例子。

3 **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（主要在数据安全法第四章）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 2019 China Business Climate Survey Report jointly released by Deloitte and AmCham China,[5] which noted that inconsistent regulatory interpretation and unclear laws and enforcement is the top challenge for 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。德勤和中国美国商会联合发布的 2019 中国商务环境调查报告[5]提到，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，也印证了这一情况。

We recommend the Commission consider:

(a) having a lead, or coordinating, regulator (eg 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;

(b) expressly specifying that the relevant lead regulator (eg PBOC) will develop detailed guidance and practical examples on how financial institutions can discharge their obligations, with:

  (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;

  (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;

(c) that rules, regulations or guidance applicable on a sectoral basis ("**sectoral rules**") should prevail over those applicable based on the location of the data activities (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 activities occur);

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

---

[5] Available at: https://www2.deloitte.com/cn/en/pages/about-deloitte/articles/deloitte-amcham-2019-china-business-climate-survey-report.html.See page 40 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。

(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.

我们建议法工委考虑下列各项：

(a) 由一个牵头或协调监管机构（如央行）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) 明确指出有关牵头监管机构（如央行）将就金融机构履行义务的方式方法制定详细指引和应用实例，包括：

(i) 采用透明及具包容性的程序，在起草阶段允许市场从业者参与（直接或通过行业协会），确保有关指引最终是切实可行且行之有效的；及

(ii) 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) 行业应用的规则、法规或指引（「**行业规则**」）的适用性应优于按数据活动所在地应用的规则（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活动所在地的地方主管机构制定的任何一般规则）；

(d) 任何金融行业新制定的行业规则应用作替代或是为明确补充现行规则而以避免范围重叠；及

(e) 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。

We would welcome the opportunity to be a part of this process.

我们十分乐意参与有关程序。

Additional comments
其他意见

We provide specific comments on some provisions in Chapter VI of the DSL in **Part B**.

我们有关数据安全法第六章若干条文的具体意见载于**乙部**。

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 is the extra-territoriality which we believe should be limited to the maximum extent possible. See our comments in paragraph 1.1 in **Part A**. The first paragraph of Article 2 clearly states that the DSL applies to all PRC Data Activities. The second paragraph raises more ambiguities. 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	**(a) Article 2 in general** We urge the Commission to re-consider and re-examine the existing National Security Law, Cybersecurity Law, 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) 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

Article 条款	Comments 意见	Recommendations 建议
	institutions. This has caused serious concerns amongst international financial institutions.	without any intent to that effect (*mens rea*). 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 1.1 of **Part A** and our comments on Article 32 in this **Part B**.
第二条	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 1.1 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。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) 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）。

Article 条款	Comments 意见	Recommendations 建议
		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 1.1 段和乙部有关第三十二条的建议。
3	The definitions of “data”, “data activities” and “data security” are too broad. In particular, the definition of “data activities” can potentially cover all aspects of commercial activities involving data.	We recommend refining the definitions such that: (a) including “impacting national security” or “safeguarding national sovereign” to the definitions of “data”, “data activities” and “data security” so as to refine the DSL’s scope of application; and (b) carving out certain purely commercial activities involving data (eg client account management and data security efforts) from the definition of “data activities”. Please also refer to our recommendations in paragraph 1.2 of **Part A**.
第三条	「数据」和「数据活动」的定义过于宽泛。 尤其是，「数据活动」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： (a) 在「数据」和「数据活动」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 (b) 将若干涉及数据的纯商业活动（如客户账户管理和数据安全工作）从「数据活动」中剔除。 亦请参阅我们在甲部第 1.2 段的建议。
4	NA	We understand that the State will establish the “data security governance system” and promote the enhancement of “data security protection capabilities”

Article 条款	Comments 意见	Recommendations 建议
		Please clarify that Article 4 does not directly apply to private entities, including financial institutions.
第四条	不适用	我们了解到，国家将建立「数据安全治理体系」，及提高「数据安全保障能力」。 建议阐明第四条不会直接应用于包括金融机构在内的私营实体。
6	It appears 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 cybersecurity and informatization department (which is responsible for the comprehensive coordination of network data security and related supervision work according to Article 7 of the 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** Financial institutions are highly regulated in many aspects. We recommend that any additional rules or regulations to be imposed on financial institutions should be at least

Article 条款	Comments 意见	Recommendations 建议
		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 paragraphs 2 and 3 of **Part A**.
第六条	从条款上看，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** 金融机构在各方面受到严格监管。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 2、3 段的建议。
7	This Article provides that the following authorities are responsible for the supervision of data security:	We make the following recommendations here: **(a) One centralised regulator** We recommend that data security of financial institutions should be supervised by a single regulator (or at

Article 条款	Comments 意见	Recommendations 建议
	(a) supervising 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.	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 0 of **Part A**. **(b) Involvement of local governments** Please clarify the local governments' involvement as referred to the first paragraph (eg 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 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.

Article 条款	Comments 意见	Recommendations 建议
		(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 a coordinator for electronic or network data. Please clarify their role, eg 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主管部门；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** 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安全，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 3 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。

Article 条款	Comments 意见	Recommendations 建议
		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	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 revise their existing rules and regulations or issue new guidelines 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 free flow of data across border; (b) the scope of cross border data transfer will be allowed (including any restrictions on the types of data);

Article 条款	Comments 意见	Recommendations 建议
		(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 33 of **Part B**; (d) the procedural requirements (eg whether entities need to undertake data security 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 3 of **Part A**. Further, we recommend the Commission to reconcile Article 10 with Article 33, including specifying the types of data which financial institutions may transfer out of the PRC without prior approval of the relevant authorities.
第十条	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，修订其现行规则和法规或颁布新指引，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

Article 条款	Comments 意见	Recommendations 建议
		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）； (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**就第三十三条提出的意见; (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 3 段的建议。 此外，我们建议法工委确保第十条与第三十三条保持一致，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。
11	NA	Please provide details of the “relevant authority” for the purpose of reporting any breach of DSL.
第十一条	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		

Article 条款	Comments 意见	Recommendations 建议
15	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. We add that the 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 different sectors and different regions in the PRC is an area of focus and concern which may deter investment.[6]	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 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 15 as follows: *"The State advances the construction of data development and use technology and data security standards systems. The State Council administrative department for*

[6] 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（只有英文版）），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（见第 6、7 页），而欧美公司对中国市场的兴趣只会令高效跨境运作更为重要。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时间，但可从报告看出业界参与者对中国市场有着强烈兴趣。

Article 条款	Comments 意见	Recommendations 建议
	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.	*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, coherence. The State creates an open and inclusive standard setting environment and supports enterprises, research institutions, institutions of higher education, related sectoral organisations, etc., 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 3 of **Part A**. **(d) Uncertainty about the legal effect of industry standards** Please clarify the nature of the standards formulated pursuant to Article 15 (eg mandatory requirements in rules or regulations, or industry recommended standards), and the implementation plan for the standards.
第十五条	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。	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

Article 条款	Comments 意见	Recommendations 建议
	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掛鈎兼容，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。	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** 我们建议对第十五条作出如下修订： *「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试试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、研究机构、高等学校、相关行业组织等参与标准制定。」* **(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 3 段详述。 **(d) 行业标准的法律效力尚不明确** 请说明根据第十五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。

Article 条款	Comments 意见	Recommendations 建议
16	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. See also our recommendation in relation to Article 20.
第十六条	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。请同时参阅我们有关第二十条的建议。
17	NA	We note that Article 17 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

Article 条款	Comments 意见	Recommendations 建议
		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.
第十七条	不适用	我们注意到，第十七条提供了政策方针。 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		
19 第十九条	We are of the view that the tiered data security system is an important part in safeguarding data security. This Articles imposes direct obligations on financial institutions. However, it is vague and lacks details on how the tiered data security system will operate.	**(a) More detailed guidance required** We recommend detailed guidance in respect of the level of protection required and the enforceability of tiered data security system. This would enable financial institutions to formulate and implement appropriate measures to ensure compliance. **(b) Whether data classification is a mandatory requirement** We refer to the guidance on classification and grading of data for security and futures industry (《证券期货业数据分类分级指引》) issued by CSRC which is a non-mandatory recommended industrial standard.

Article 条款	Comments 意见	Recommendations 建议
		This CSRC guidance provides for a multi-level data protection scheme conducted at an industry-specific level. Please clarify whether the tiered data security system under this Article requires financial institutions to perform data grading and classification as a mandatory legal requirement. Furthermore, financial institutions are already subject to various regulations and any additional standardisations and categorisations should be avoided so as to reduce possible overlaps and inconsistencies.
	我们认为，数据安全分级制度是保护数据安全的重要一环。 本条对金融机构施加直接义务。然而，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。	**(a) 需要更详细的指引** 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制定详细指引，令金融机构能够制定和实施适当的措施，确保合规。 **(b) 是否强制需为数据分级分类** 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。 本条下的数据安全分级制度要求金融机构进行数据分级和分类，请说明有关要求是否属强制性的法律要求。此外，金融机构现时须遵守若干法规，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。
	There may be inconsistent definitions of “important data”. The DSL does not define “important data”, instead it delegates each relevant regional and departmental authorities to regulators to	**(a) Define “important data” in the DSL** We submit that the definition of “important data” should be consistent across regardless of the location of the data activities and industry in respect of which the data is used.

Article 条款	Comments 意见	Recommendations 建议
	formulate a catalogue of "important data". 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.	We also request the Commission to clarify whether "important data" will form part of the "controlled categories" referred to in Article 23. **(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. 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 catalogues. **(c) Involving market participants in drafting of the definition of "important data"** We request relevant sector regulatory 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 of **Part A**.

Article 条款	Comments 意见	Recommendations 建议
		This is particularly important as Articles 25 and 28 of the DSL impose various data security protection obligations on financial institutions and their responsible persons and the management body. See also our comments on Article 25. **(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) ("Guidance"); and ▪ the draft Financial Data Security – Guides of Data Security Classification (2020) ("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. **(e)** 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」，而是授权各地区、各部门确定「重要数据」保护目录。	**(a) 数据安全法对「重要数据」的定义** 我们认为，不论开展数据活动的地点和使用数据的行业，「重要数据」的定义应保持一致。 我们请求法工委阐明「重要数据」是否属于第二十三条所述的「管制物项」类别。

Article 条款	Comments 意见	Recommendations 建议
	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。	**(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，而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** 我们请求有关行业监管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 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。 这对数据安全法第二十五、二十八条尤为重要，有关条款对金融机构、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二十五条的有关意见。 **(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： ▪ 《数据出境安全评估指南（草案）》(2017 年)(「**评估指南**」)；及

Article 条款	Comments 意见	Recommendations 建议
		▪ 《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。 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。
20	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 (eg 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, 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.

[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.（只有英文版）

Article 条款	Comments 意见	Recommendations 建议
第二十条	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、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》。
22 第二十二条	**(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 assess its impact on their business operations and their risks.	We recommend: ▪ providing more details on what the data security review system will entail and how it will be implemented; ▪ 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 (eg 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

Article 条款	Comments 意见	Recommendations 建议
		▪ that the Commissioner 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 activities", we are concerned that this Article may lead to an unintendedly broad interpretation and application.	We recommend clarifying how the data security review in this Article relates to the "security assessment processes" described in the Cybersecurity Law, the data security risk assessment (as stated in Article 20), 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.
	(b) 潜在应用范围较广 鉴于「数据活动」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所述的「安全评估程序」、数据安全风险评估（见第二十条）、国信办颁布的指引草案以及各项行业标准相互联系。

Article 条款	Comments 意见	Recommendations 建议
		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。
23	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 draft 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".
第二十三条	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： (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。	我们建议阐明本条所述的「管制物项」是否是指《出口管制法（草案）》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」。

Article 条款	Comments 意见	Recommendations 建议
	(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。	
24	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 (d) the specific circumstances and data types to which this Article 24 may apply.
第二十四条	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 (d) 本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 3 of **Part A**.

Article 条款	Comments 意见	Recommendations 建议
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 3 段。
25 第二十五条	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 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 15), 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（如我们在有关第十五条的建议中所述，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。

Article 条款	Comments 意见	Recommendations 建议
	(b) Responsible person and management body for data security This Article imposes direct obligations on private entities to maintain responsible personnel and management body for the purpose of the data security protection. However, no detailed guidance has been provided as to complying with these requirements.	To enable financial institutions to comply, we recommend expressly clarifying: ▪ that the responsible person can share roles between group companies or other similar data protection roles under other laws or regulations; ▪ that the responsible person can have other roles; and ▪ the obligations and potential liabilities of the responsible person and the management body.
	(b) 数据安全的负责人和管理机构 本条对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： ▪ 负责人可根据其他法律法规在集团公司之间分担职责或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。
27	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 27 to be interpreted properly. We also suggest 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 (eg under contract). Such guidance should assist

Article 条款	Comments 意见	Recommendations 建议
		financial institutions to navigate those conflicting obligations.
第二十七条	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，让本条得以适当解读。 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。
28	NA	We refer to our comments on Article 19 with respect to the definition of "important data". Please clarify the triggering event for a financial institution to conduct data risk assessments and provide 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.
第二十八条	不适用	谨此提述我们关于第十九条下对「重要数据」定义的意见。 请列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。
29	NA	We recommend amending Article 29 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~~*

Article 条款	Comments 意见	Recommendations 建议
		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, and may not exceed the limits of necessity~~ intended purpose." We also recommend clarifying the ambit of "data collection" in this Article.
第二十九条	不适用	我们建议对第二十九条作出如下修订： *「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。
30	NA	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 is 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.

Article 条款	Comments 意见	Recommendations 建议
		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. We also suggest the Commission to consult the relevant authorities, and industry stakeholders to ensure that they are practicable and workable. 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 3 of **Part A**.
第三十条	不适用	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监管监督，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大笔费用和繁杂工作。新规定与现行规定之间的相互影响也可能为数据当事人带来意料之外的后果。我们建议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

Article 条款	Comments 意见	Recommendations 建议
		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。 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 3 段的意见。
31	NA	We make the following recommendations here: **(a) Scope of the licensing regime for "specialised online data processing services"** We recommend defining "specialised online data processing services" to clarify the scope of the licensing regime. We further submit that foreign entities should also be eligible for the licence to operate "specialised online data processing 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.
第三十一条	不适用	我们的建议如下： **(a) 「专门的在线数据处理服务」的经营许可颁发制度范围** 我们建议界定「专门的在线数据处

Article 条款	Comments 意见	Recommendations 建议
		理服务」，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「专门的在线数据处理服务」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。
32	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 (eg 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	We recommend providing specific details regarding: (a) the relevant laws and regulations referred to in Article 32 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.

Article 条款	Comments 意见	Recommendations 建议
	not cover non-PRC Data Activities. See also our comments on the DSL's extraterritoriality in paragraph 1.1 of **Part A**.	
第三十二条	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 1.1 段我们有关数据安全法域外法权的意见。	我们建议就下列各项补充具体说明: (a) 第三十二条所述，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。
33	We refer to Article 177 of the Securities 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 law enforcement bodies.	We 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;

Article 条款	Comments 意见	Recommendations 建议
	We submit that this expansion will create major issues for global financial institutions 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.	(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 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 or reporting for anti-money laundering and counter-terrorism financing purposes; or (e) to provision of data to international organisations (eg Interpol). 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 10.
第三十三条	据我们所知，《证券法》第一百七十七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，目前的情况是建议将有关范围扩大至涵盖境外执法机构要求提供的在中国存储的一切数据。 我们认为，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，	我们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（即在境外执法机构要求提供数据前，已在有关中

Article 条款	Comments 意见	Recommendations 建议
	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。	国境外的司法管辖区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。 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条的建议。
Chapter V Government Data Security and Openness 第五章 政务数据安全与开放		
39	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. However, we are concerned whether financial institutions have lost their rights over the data they collected if they aggregate or combine with government data.	In this regard, we recommend defining "government data" and providing more details on how the ownership of data may be affected if the government data is combined with the data collected by the financial institutions.
第三十九条	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	就此而言，我们建议界定「政务数据」的涵义，更具体说明如政务数据与金融

Article 条款	Comments 意见	Recommendations 建议
	金融和可持续发展有着关键作用。 可是，我们关心如果金融机构收集的数据与政务数据合并，金融机构是否会失去其对该等数据的权利。	机构收集的数据合并会对数据的所有权造成怎样的影响。
41	NA	Please clarify the criteria in finding a "material security risk in data activity".
第四十一条	不适用	请列明发现「数据活动存在较大安全风险」的标准。
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。
46	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.
第四十六条	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	我们建议对本条作下列修改：

Article 条款	Comments 意见	Recommendations 建议
	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。	*「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。
47	We believe that the penalty provisions in the respective laws and regulations are sufficient. We are also concerned that a generic cross-reference to other crimes which are already covered in other laws may cause confusion.	We recommend providing more specificity to this Article by including: ▪ express reference to relevant penalty provisions; ▪ taking into account other penalty regimes; and ▪ a roadmap for enforcement in the case of overlapping issues.
第四十七条	我们认为，相关法律法规内的处罚规定已足够。 我们担心对其他法律已涵盖的其他罪行作一般参照可能会引起混淆。	我们建议在本条内作更详细的说明，包括： ▪ 说明会参照有关处罚规定； ▪ 将其他处罚制度纳入考量；及 ▪ 在出现重叠问题的情况下所采用执行程序。
49	We believe the existing Law on Guarding State Secrets is sufficient in regulating data that constitute state secrets.	We recommend expressly stating that the DSL does not govern data that constitutes a state secret or which relates to the military.
第四十九条	我们认为，现行的《保守国家秘密法》足以规管构成国家秘密的数据。	我们建议明确指出数据安全法不适用于构成国家秘密或与军事有关的数据。