19 November 2020
2020 年 11 月 19 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 Personal Information Protection Law

《个人信息保护法》征求意见稿

On behalf of its members, the Global Financial Markets Association ("**GFMA**")[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 Personal Information Protection Law ("**PIPL**") of the People's Republic of China ("**PRC**") published on the National People's

---

1 The Global Financial Markets Association ("**GFMA"**) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London and Brussels, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, please visit http://www.gfma.org .

GFMA 汇集了三个世界领先的金融贸易协会，以应对日益重要的全球监管议程，并促进协调一致的倡导工作。位于伦敦和布鲁塞尔的欧洲金融市场协会（AFME）、位于香港的亚洲证券业和金融市场协会（ASIFMA）以及位于纽约和华盛顿的证券业和金融市场协会（SIFMA）分别是 GFMA 欧洲、亚洲和北美的成员。更多信息请访问 http://www.gfma.org

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

Congress website[3].

全球金融市场协会（“**GFMA**”）及期货行业协会（“**FIA**”）（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（“**中国**”）个人信息保护法（“**个人信息保护法**”）》征求意见稿向第 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。

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

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个人信息保护法的意见、金融机构可能面临的实际困难、我们的建议以及我们对个人信息保护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 personal information. Personal information is pivotal to the business of our members, and concomitant protections on the collection and processing of such information are essential to the integrity of financial markets and customer, 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个人信息的需要。个人信息不仅是本协会成员进行业务经营的关键，在收集和处理此类信息的同时提供相应保护，对于健全金融市场及稳定消费者和经营者信心也至关重要。

At the same time, the PIPL casts a broad net. In certain instances, the new law is difficult to interpret in practice and could be open to interpretation where possibly unintended. Its interaction with existing legal and regulatory requirements and expectations – in particularly the Cybersecurity Law (“**CSL**”) and the Data Security Law (draft) (“**DSL**”) – is also unclear.

同时，个人信息保护法涵盖范围广泛。在部分情况下，新法律难以作出具体解释或在无意的情况下可以有各种不同的解读。个人信息保护法与现有法律法规的要求和期望 – 尤其是《网络安全法》（“**网络安全法**”）和《数据安全法（草案）》（“**数据安全法**”）之间的关系和相互影响尚不明朗。

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

---

[3] Available at: http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808175265dd401754405c03f154c. 可于以下网址查阅：http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808175265dd401754405c03f154c.

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

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

(ii) Onerous obligations on organisations including financial institutions will significantly raise their compliance burden, in particular in respect of cross-border transfers of personal information and collecting and processing personal information legally.

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

(iv) Principle-based obligations which will require more specific guidance to enable compliance in practice and this guidance should be available from before any compliance requirements become effective.

个人信息保护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，目前个人信息保护法草案措词宽泛，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) 个人信息保护法的广泛应用范围及其域外适用问题。

(ii) 对包括金融机构在内的组织而言，繁重的义务将大幅增加其合规负担，特别是在跨境转移个人信息和合法收集和处理个人信息方面。

(iii) 与现行法律法规重叠。尤其是，金融机构开展的个人信息处理活动受到高度监管，因此，在个人信息保护法实施前厘清法律重叠的范围或分歧，十分关键。

(iv) 原则性义务的实际遵守需要更具体的指引并且该指引应在任何合规要求生效之前提供。

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 among our members. They include:

(i) the broad range of processing activities in Article 3 including, in particular, the extraterritorial scope of the activities caught under this Article and Article 42;

(ii) the lack of business-efficient processing conditions under Article 13;

(iii) the requirement to obtain "separate" consents from individuals in certain scenarios under Article 14, 24, 26, 27, 30 and 39;

(iv) the restrictions on the cross-border transfers of personal information in Article 38 and 40;

(v) the framework outlined for risk assessments in Article 54; and

(vi) the significant financial sanctions imposed on organisations and individuals under Chapter VII.

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) 第三条中的处理活动范围宽泛，尤其是包括根据本条和第四十二条进行的活动的域外范围；

(ii) 缺乏第十三条所规定的有效业务处理条件；

(iii) 根据第十四条、第二十四条、第二十六条、第二十七条、第三十条和第三十九条的规定，在某些情况下须获得个人的"单独"同意；

(iv) 第三十八条和第四十条对个人信息跨境转移的限制；

(v) 第五十四条概述的风险评估框架；及

(vi) 根据第七章对组织和个人实施的重大金融制裁。

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 Zhao Sheng Linklaters (FTZ) Joint Operations Office, based on feedback from the wider ASIFMA membership.

本函件在昭胜年利达（上海自贸区）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！

Kenneth E. Bentsen, Jr.
CEO, Global Financial Markets Association (GFMA) and
President and CEO, Securities Industry and Financial Markets Association (SIFMA)

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 PIPL, and any reference to the "**PIPL**" is a reference to the draft PIPL 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个人信息保护法赋予其的涵义，并应根据本函件或个人信息保护法解释。"**个人信息保护法**"指截至本函件日期在中国人大网所登载的个人信息保护法草案。

Part A Overarching comments

甲部 整体意见

1 Scope of application: Extra-territoriality
应用范围：域外法权

We appreciate that the purpose of the PIPL is to create a framework for protection of personal information rights and interests, regulating personal information processing activities, safeguarding the orderly sharing and transfer of personal information, and promoting the reasonable use of such information in a growing digital economy. However, the potential reach of the PIPL may cause unnecessary burden to international financial institutions.

我们认同个人信息保护法的目的是建立一个保护个人信息权益的框架，规范个人信息处理活动，维护个人信息的有序共享和转移，并在不断发展的数字经济中促进此类信息的合理使用。然而，个人信息保护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。

The PIPL covers:

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

(b) certain data activities conducted by organisations or individuals outside the PRC, including those who seek to provide products or services into the PRC or monitor the activities of individuals within the PRC, or whose processing activities conducted outside the PRC harm the personal information rights and interests of PRC citizens or the national security or public interest of the PRC ("**Non-PRC Data Activities**").

个人信息保护法涵盖：

(a) 在中国境内开展的数据活动（"**中国境内数据活动**"）；及

(b) 中国境外的组织或个人开展的若干数据活动，包括寻求向中国提供产品或服务或监视中国境内个人活动的数据活动，或者在中国境外开展的处理活动损害中国公民的个人信息权益或中国的国家安全或公众利益的数据活动（"**中国境外数据活动**"）。

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

我们的理解是，个人信息保护法拟适用于一切中国境内数据活动，并对中国境外数据活动依法追究法律责任。

We strongly urge that the PIPL focuses on PRC Data Activities. In particular, the provisions in the PIPL, whereby any personal information processing activities conducted outside the PRC which harm the personal information rights and interests of PRC citizens or the national security or public interest of the PRC, 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 the business community.

我们强烈促请个人信息保护法围绕中国境内数据活动制定。尤其是，个人信息保护法中关于在中国境外开展的任何个人信息处理活动若损害中国公民的个人信息权益或中国的国家安全或公众利益的条款，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，因此金融机构及整个业界极为关注。

Having regard to the strategic importance of personal information, 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 PIPL will be applied and enforced in practice, particularly, with respect to foreign entities which do not have physical presence in the PRC.

---

[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 PIPL.

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，与我们所理解的个人信息保护法的定义一致。

考虑到个人信息的战略重要性、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个人信息保护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 PIPL is too broad and uncertain in its extra-territorial reach. More specifically, the application of the PIPL to activities of organisations and individuals 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. 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.

首先，我们认为个人信息保护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，如果中国境外的组织和个人无法以明确客观参数合理地作出评估，那么中国境外的组织和个人将难以应用个人信息保护法于其开展的活动。根据草案，域外应用范围尤为繁重，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。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。

Furthermore, as noted above, the PIPL's jurisdictional reach also exceeds that of the CSL. We submit that the extra-territorial application of the existing CSL is sufficient to protect safeguard national security. The very fact of the difference in jurisdictional reach of the PIPL and the CSL creates a degree of complexity that has already caused serious concerns amongst foreign financial institutions. We believe restricting the PIPL'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. See also our comments in paragraph 4.

此外，如上文所述，个人信息保护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，个人信息保护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，将个人信息保护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 4 段提出的意见。

Finally, where certain provisions are *not* intended to apply to personal information processing activities conducted outside the PRC, the PIPL 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 personal information protection obligations set out under the PIPL. It would be preferable to exclude Non-PRC Data Activities expressly from those personal information protection obligations.

最后，如果*无意*对中国境外开展的个人信息处理活动应用部分条文，则个人信息保护法应作出明确排除，以免除对有关事宜的疑问。例如，要求境外实体履行个人信息保护法所载列的所有个人信息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个人信息保护义务之外，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 PIPL will be enforced in practice, in terms of:

(a) communicating standards and expectations;

(b) undertaking investigations; and

(c) levying penalties.

我们欢迎对个人信息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 comments

具体意见

We provide specific comments on Articles 10, 11, 42, 57, 58 and 59 of the PIPL in **Part B**.

我们有关个人信息保护法第十条、第十一条、第四十二条、第五十七条、第五十八条和第五十九条的具体意见载于**乙部**。

2 Data localisation and cross-border transfers of personal information 数据本地化和个人信息跨境传输

Another critical part of the regime set out under the PIPL is that relating to data

localisation and cross-border transfers of personal information.

个人信息保护法项下制度的另一个关键部分涉及到数据的本地化及个人信息跨境传输。

The localisation requirements proposed under the PIPL 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. Burdensome 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.

个人信息保护法项下提出的本地化要求，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。

The prospect of additional security assessments by regulatory authorities or third-party certification institutions for potentially every cross-border transfer of personal information will lead to increases in compliance administration and costs to the detriment of customers and, ultimately and contrary to the PRC government's commitments to open up the financial services sector, make the PRC market less attractive to overseas financial institutions.

监管机构或第三方认证机构对每一次潜在的个人信息跨境传输进行额外的安全评估将导致客户接受更多合规管理，并承担更多费用，并最终导致中国市场对海外金融机构的吸引力减少，这也有悖于中国政府的开放金融服务领域承诺。

We urge the Commission to consider a more proportionate approach to supervision of exports of personal information considering the existing laws and regulations already governing this aspect of data use. Specifically, we recommend removing the requirement that "processors processing personal information above a certain threshold" must store data within the PRC. However, where requirements are considered necessary in addition to those under existing laws and regulations, we recommend that an exception is expressly provided for intra-group transfers as global financial institutions apply uniform levels of data security on a firm-wide basis, where transfer restrictions are considered appropriate at an industry level provided that risk is adequately mitigated.

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个人信息出境采取更为合适的监管方式。特别是，我们建议删除关于“个人信息处理者所处理的个人信息超过规定数量”就必须将数据存储在境内的要求。但是，如除

现行法律法规外，还有必要提出其他要求，则我们建议，如果在行业层面认为适用出境限制以充分降低风险，则应对同一集团内部的数据出境明确作出例外性规定，原因是，跨国金融机构在集团内部均适用统一的数据安全水准。

Additional comments

具体意见

We provide specific comments on Chapter IV of the PIPL in **Part B**.

我们有关个人信息保护法第四章的具体意见载于**乙部**。

3 Processing grounds
处理依据

We strongly welcome the introduction under the PIPL of other statutory processing grounds to obtaining consent of a data subject to be able to collect and process his or her personal information. However, we also believe that the scope of alternative processing grounds lacks a number of conditions important to financial institutions and other businesses from a business efficacy perspective. For example, the PIPL does not include processing grounds relating to processing of personal information that is essential for maintaining safe and stable operation of products and services and processing of personal information already legally in the public domain (both of which are included in the Information security technology: personal information security specification (GB/T 35273-2020) (the "**2020 Specification**").

我们非常欢迎个人信息保护法下引入取得数据主体同意以收集和处理其个人信息的其他法定处理依据。但是，我们也认为从业务效效益角度来看，备选的处理依据范围缺乏对金融机构和其他企业很重要的一些条件。举例而言，个人信息保护法并无包括关于处理对维护产品和服务的安全稳定运行所必需的个人信息以及处理在法律上已经属于公有领域的个人信息的处理依据（上述两种个人信息已包含在《信息安全技术个人信息安全规范》（GB/T 35273-2020）（"**2020 年规范**"））。

In addition to allowing reasonable flexibility in the collection and processing of personal information, we are concerned about the apparent inclusion of a number of scenarios that require financial institutions to obtain "separate" consents from individuals – namely under Articles 14, 24, 26, 27, 30 and 39.

除了在收集和处理个人信息方面给与合理灵活性外，我们也关注到个人信息法明显包括了一些要求金融机构从个人获得"单独"同意的情况 – 见第十四条、第二十四条、第二十六条、第二十七条、第三十条和第三十九条。

Firstly, the meaning of a "separate" consent is unclear under the current form of the PIPL, so compliance with the requirement would be difficult for financial institutions which already have in place robust customer onboarding and other interface processes to ensure customers are properly informed on the products and services offered to them. Furthermore, not only is this additional burden highly impractical for businesses in the finance sector (and other consumer

sectors) if it cuts across the processing grounds described above but, rather than empowering individuals in the protection of their personal data, there is reason to believe that frequently seeking consents from customers would unnecessarily damage their customer experience. In addition, if an organisation is beholden to a "just in time" consent requirement, these articles could create an operational challenge and we recommend consent be obtained at the point of collection or disclosure of personal information. Repository maintenance of multiple consents will create additional concerns.

首先，在个人信息保护法的目前版本下，“单独”同意的含义并不清晰，因此，对于建立了健全的客户登记和其他接口流程，以确保客户能够正确了解向他们提供的产品和服务的金融机构来说，遵守这一要求将是困难的。此外，如果超出上述处理依据，这一额外负担不仅对金融业（和其他消费行业）的企业来说是非常不切实际，而且有理由相信，频繁地寻求客户同意会不必要地损害他们的客户体验，而不是赋权个人保护其个人资料。另外，如果某个组织须遵守“及时”同意要求，则该等规定可能会带来操作上的困难。我们建议在收集或披露个人信息时，即应取得同意。对多项同意的存储和维护也会产生其他问题。

We recommend that the PIPL avoid establishing consent (in any form) as the primary legal basis for collecting, using, disclosing or otherwise processing personal information, including its cross-border transfer. Consent, as it is proposed in the PIPL, creates a degree of legal uncertainty as consent is always capable of being withdrawn. This uncertainty creates inherent operational and compliance issues which could be avoided if other legal grounds for processing are treated as equally legitimate alternatives to consent. For these reasons, we urge the Commission to adopt the concept of "legitimate interests" of the processor as an additional processing ground, which requires the processor to balance the risk associated with a particular processing activity with the rights and interests of the data subjects. As such, the Commission should reconsider how consent should work in practice and, indeed, whether it is necessary in light of the protections for individuals that already exist under various laws and regulations at national and industry levels.

我们建议，个人信息保护法应避免将（任何形式的）同意作为收集、使用、披露或以其他方式处理个人信息（包括跨境转移）的主要法律依据。如个人信息保护法中所提议，同意会造成一定程度的法律上的不确定性，因为同意总是可以撤回的。这种不确定性将一定会带来运营和合规方面的问题，但如果将信息处理的其他法律依据视为可以取代同意的同等合法选择，则可以避免这些问题。鉴于这些理由，我们促请法工委采用处理者的“合法权益”概念作为额外的处理依据，这要求处理者在与特定处理活动相关的风险与数据主体的权益之间取得平衡。因此，法工委应重新考虑这一同意要求在实践中应如何发挥作用，以及在各部全国性和行业性的法律、法规下已对个人提供的保护的情况下，这一同意要求是否还有必要。

Additional comments

具体意见

We provide specific comments on Chapter IV of the PIPL in **Part B**.

在**乙部**中我们对个人信息保护法第 13 条的评论中，可以看到合法权益如何运作的具体示例。

4 Overlap with other laws
与其他法律重叠

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

个人信息保护法的应用范围广泛，导致与现行法律、法规和指引的应用范围重叠。

For example, the 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 amongst the PIPL, the 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. 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"*。如果个人信息保护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 PIPL will interact with these laws.

因此，我们希望能够阐明个人信息保护法将如何与该等法律相互作用，并就此作出详细指引。

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

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) 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

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) the **DSL**, for which the first public consultation process was completed on 16 August 2020.

数据安全法，该法于 2020 年 8 月 16 日结束首次公开征求意见。

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

我们建议调整个人信息保护法的范围，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):

此外，我们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 PIPL interacts with other laws, regulations or guidelines.

个人信息保护法如何与其他法律、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 PIPL, and to discuss with the relevant authorities with a view to harmonising the PIPL with the other laws, regulations and guidelines. For example, other than the Cyberspace Administration of China ("**CAC**"), the People's Bank of China ("**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.

我们促请法工委优先检视可能会与个人信息保护法重叠的相关法律、法规和指引，与有关主管机构探讨如何令个人信息保护法与其他法律、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**"）、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。

Additional comments

具体意见

See a specific example of how the PIPL may overlap in our comments on Article 13 of the PIPL in **Part B**.

乙部载有我们就个人信息保护法第十三条提出的意见，当中列举有关个人信息保护法可能如何与现行法律法规重叠的具体例子。

5 Principle-based obligations
原则性义务

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

我们知悉，个人信息保护法载有一般性原则，并预期相关主管机构会制定进一步的细则。

That said, certain provisions 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 PIPL 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个人信息保护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 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。德勤和中国美国商会联合发布的 2019 年中国商务环境调查报告提到，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:

我们建议法工委考虑下列各项：

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

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个人信息保护法，包括就个人信息保护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；

---

[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。

(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:

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 and remain 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且一直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 PIPL are consistently implemented by each sector, and reduce the likelihood of regulatory arbitrage;

通过各主管机构合作，确保个人信息保护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 applicable based on the location of personal information processing 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 processing activities occur);

按行业应用的规则、法规或指引（"**行业规则**"）的适用性应优于按个人信息处理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信息处理活动所在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用作替代或是为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 PIPL, 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 PIPL, 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.

行业规则与个人信息保护法同时生效，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个人信息保护法同时生效，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

具体意见

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

我们有关个人信息保护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 PIPL.

除**甲部**的意见外，下表概述我们有关个人信息保护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**		
3	**(a) Location of individuals protected** The PIPL applies to the "personal information of natural persons in the People's Republic of China". We assume this applies to the personal information of all persons physically within the borders of the PRC rather than being limited to Chinese nationals. However, unlike under the draft of the Information Security Technology - Guidelines for Cross-Border Data Transfer Security Assessments issued by the National Information Security Standardisation Technical Committee in August 2017 (the "**2017 Cross-Border Transfer Guidelines**") there is no clarification on whether personal information on persons outside of the PRC is regulated – for example, personal information transferred through the PRC where such information is not collected or generated in the PRC and not changed or processed in the PRC; or personal information that is not collected or generated in the PRC, even though such information is stored or processed in the PRC. **(b) Broad scope of "analyse or assess" as processing activities** We submit that the current concept of "analyse or assess the behaviour of natural persons in the PRC" under item 2 of Article 3 is extremely broad, such as may include a wide range of activities that are not intended to be in scope of the	**(a) Clarify scope of individuals who are protected** We recommend that the PIPL or implementing regulations to be published at the time of promulgation of the PIPL clarify the scope of individuals whose personal information is intended to be regulated under the PIPL. **(b) Narrowing down the scope of "analyse or assess"** We recommend narrowing the scope of item (2) to "using big data analytics to analyse and assess the behaviour of natural persons in PRC for profiling purposes" to avoid unintentionally catching legitimate operational needs of multinational financial institutions. **(c) Deletion of catch-all provision** We urge that the PIPL focuses on PRC processing activities to the extent possible to avoid an expansive application of the PIPL that conflicts with the legal obligations of enterprises operating on a cross-border basis, such extraterritoriality being of serious concern to the international business community. To the extent that extraterritorial reach is required, the scope of application should be clearly designated for enterprises and individuals. In particular, whereas the concepts set out in this article are like

Article 条款	Comments 意见	Recommendations 建议
	PIPL. For example, if read literally, the PIPL may also apply to persons reading legitimate news reports about natural persons based in the PRC. However, we understand that such circumstance is not contemplated as being a regulated activity given the exemption under Article 5.6(h) of 2020 Specification. **(c) Catch-all provision** We also submit that the current "catch-all" at item 3 of Article 3 prescribes for very broad interpretation and creates uncertainty which could result in conflicting legal obligations with respect to processing activities of financial institutions outside of China. The similar provision under Article 3 of the GDPR does not provide for such a catch-all and we urge that the Commission considers a similar approach given the clear sensitivity that such extraterritoriality would have for international financial institutions. **(d) Wide application of PIPL** Though Article 68 excludes certain activities conducted by individuals, the PIPL generally applies to both organisations and individuals. The California Consumer Privacy Act (CCPA), for example, only applies to for-profit businesses that do business in California and meet certain conditions (1798.140). **(e) Lack of clarity on deceased persons** It is unclear whether the PIPL applies to the personal information of deceased persons. The GDPR, for example, clarifies in the recitals to the regulation that it does not apply to deceased individuals.	those under the GDPR, the GDPR and its implementing rules and supporting caselaw seek to provide further detail on, for example, when an overseas business operator could be seen as offering goods and services in the EU. The implementing rules of the GDPR further discuss 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. We urge that the PIPL must prescribe similar indications as to the extent of its extraterritorial application on the offering of goods or services. **(d) Reduction in scope of relationships regulated** We recommend that the persons regulated under the PIPL should be limited to organisations. Individuals, business and commercial relationships should not be regulated by the PIPL. **(e) Clarification on deceased natural persons** We recommend clarifying whether the PIPL applies to the personal information of deceased persons.
第三条	**(a) 受保护个人的地点**	**(a) 明确受保护个人的范围**

Article 条款	Comments 意见	Recommendations 建议
	个人信息保护法适用于“中华人民共和国境内自然人个人信息”。我们假设这适用于在物理上位于中国境内的所有人的个人信息，而不仅限于中国公民的个人信息。但是，与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（**“2017 年数据出境安全评估指南”**）相比，个人信息保护法对于中国境外人士的个人信息是否受到监管的问题，尚未作出澄清 – 例如，通过中国转移但既未在中国境内收集或产生也未在中国境内更改或处理的个人信息；或在中国境内存储或处理的非在中国境内收集或产生的个人信息。 **(b) “分析或评估”作为处理活动的范围的宽泛性** 我们认为，目前第三条第（二）项下关于“为分析、评估境内自然人的行为”的概念过于宽泛，例如可能包括那些并非意图纳入个人信息保护法范围的各种活动。例如，从字面上看，个人信息保护法也可能适用于阅读关于中国境内自然人的合法新闻报道的人。但是，我们理解，鉴于 2020 年规范第 5.6（h）条项下的豁免规定，这种情况不被视为受监管活动。 **(c) 总括性条款** 我们还认为，目前第三条第（三）项中的总括性规定有非常宽泛的解释空间并创造了不确定性，可能会导致与金融机构在中国境外的处理活动有关的法律义务发生冲突。GDPR 第 3 条项下的类似规定并未有这种概括性的规定，考虑到该等域外法权对于国际金融机构而言有明显的敏感性，我们促请法工委考虑采取类似做法。 **(d) 个人信息保护法的宽泛适用** 尽管第六十八条排除了个人进行的某些活动，但个人信息保护法总体上同时适用于组织和个人。	我们建议，在颁布个人信息保护法时所发布的个人信息保护法或实施细则应明确其个人信息将受到个人信息保护法项下监管的个人的范围。 **(b) 缩小“分析或评估”的范围** 我们建议将第（二）项的范围缩小为“以为用户画像为目的使用大数据分析法分析和评估中国境内自然人的行为”，以避免无意间妨碍跨国金融机构的合法运营需求。 **(c) 删除总括性条款** 我们认为，个人信息保护法应尽可能地聚焦于中国境内的处理活动，以避免因个人信息保护法的广泛适用导致与跨境运营的企业的法律义务相抵触，而国际商界对这种域外法权是严重关切的。 如果域外适用具有必要性，则应为企业和个人明确指定适用范围。尤其是，尽管本条中所列出的概念与 GDPR 项下的概念相类似，但 GDPR 及其实施细则和配套的判例法致力于提供更多细节规定，例如，对关于何时可将某一海外经营者视为在欧盟提供商品和服务作进一步规定。GDPR 的实施细则进一步讨论了域外法权如何仅针对有意、有针对性地向欧盟境内个人提供商品或服务的行为，而非针对偶然地或无意地提供商品或服务的情况。我们建议，个人信息保护法须就其在域外适用于提供商品或服务的程度作出类似的规定。 **(d) 减少受监管的关系的范围** 我们建议，受个人信息保护法监管的人士应仅限于组织。个人、业务和商业关系不应受到个人信息保护法的监管。 **(e) 对本法是否适用于已故自然人作出规定** 我们建议就个人信息保护法是否适

Article 条款	Comments 意见	Recommendations 建议
	例如，《加州消费者隐私保护法》（CCPA）仅适用于在加州开展业务并满足某些条件的营利性企业（加州民法第1798.140条）。 **(e) 对死者的个人信息是否保护尚不明确** 尚不清楚个人信息保护法是否适用于死者的个人信息。例如，GDPR 在该条例的鉴于条款中阐明了该条例不适用于已故的个人。	用于已故自然人的个人信息作出规定。
4	The definition of “personal information” is narrower than the equivalent definition under Article 76 of the CSL which additionally refers to various information “used alone or in combination with other information to recognise the identity of a natural person” and gives a number of express examples. This difference in the definitions may be confusing for the enterprises to apply in practice. We agree that the definitions of “processing” and “personal information” could be broad, if precisely set out. However, we strongly believe that inclusive definitions like that of “processing” and terms like “other such activities”, if not precisely defined, should be avoided, as they are very difficult to apply in practice and carry a high risk of inconsistent application.	**(a) Resolve the discrepancy in definition of “personal information”** We recommend aligning the definition of “personal information” to that under the CSL. **(b) Narrow the definition of “processing”** We recommend that any additional activities that the government views as constituting processing should be expressly set out in the definition.
第四条	“个人信息”的定义相比网络安全法第七十六条中的定义要窄，网络安全法中“个人信息”的定义包括了“单独或者与其他信息结合识别自然人个人身份”的各种信息，并列举了许多例子。定义方面的这一差异可能会导致企业在实践中适用时感到困惑。 我们同意，如果作出明确规定的话，“处理”和“个人信息”的定义可能会很宽泛。但是，我们坚决认为，如果没有明确定义，则应避免使用包容性定义(如“处理”的定义)和诸如“等活动”之类的表述，因为在实践中它们很难适用，且存在	**(a) 解决“个人信息”定义不一致问题** 我们建议将“个人信息”的定义与网络安全法项下的定义保持一致。 **(b) 缩小“处理”的定义范围** 我们建议在定义中明确列出政府认为构成处理的任何其他活动。

Article 条款	Comments 意见	Recommendations 建议
	适用不一致的很大风险。	
9	It is unclear what “necessary measures” should be adopted to safeguard the security of the personal information.	We recommend clarifying the “necessary measures” that the personal information processors should adopt and whether this includes compliance with industry standards as opposed to only mandatory requirements.
第九条	不清楚应采取哪些“必要措施”来保障个人信息的安全。	我们建议应写明个人信息处理者应采取的“必要措施”，并明确这些措施是否包括遵守行业标准，而非仅遵守强制性要求。
10	The DSL is formulated, among others, to safeguarding state sovereignty and national security (according to article 1 of the DSL). Therefore, the prohibition on organisations and individuals to process personal information in a manner which is prejudicial to “national security or public interests” overlaps with obligations provided under the DSL. The reference to “administrative regulations” 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 therefore expand the scope of application of those standard and uplift the punishment for existing requirements. We believe the original intention of those requirements should be upheld.	**(a) Omit overlapping concepts** We are of the view that the DSL is the better law to deal with matters of national security or public interest and therefore this article of the PIPL is unnecessary and should be deleted to avoid creating confusion through overlapping obligations. This is a more general issue that should be addressed through the DSL. **(b) Application of non-mandatory requirements** Furthermore, we recommend expressly clarifying that: • processing activities should only need to be conducted in compliance with mandatory requirements under relevant laws and regulations; and • entities will not be required to strictly adopt recommended standards or best practices (which should be in line with international standards as mentioned in our recommendation on Article 11), but there should be a degree of discretion as to the standards or practices followed to allow entities to comply with or go beyond the mandatory requirements under the PIPL.
第十条	数据安全法的立法目的之一是为了维护国	**(a) 删除重复性概念**

Article 条款	Comments 意见	Recommendations 建议
	家主权和国家安全（根据数据安全法第一条）。因此，禁止组织和个人从事危害“国家安全、公共利益”的个人信息处理活动的规定，与数据安全法所规定的义务存在重叠。 提到“行政法规”可能会起到超出初衷的效果，即要求私人实体严格遵守推荐性标准，而这些标准原本是没有法律效力的。因此，本条有可能扩大这些标准的适用范围，并提高对违反现有要求所作的处罚。我们认为这些要求的初衷应得以维护。	我们认为，数据安全法是处理国家安全或公共利益事务的更好的法律，因此，个人信息保护法中这一条没有必要作出重复规定，应予删除，以免因义务重叠而造成困扰。这是一个更一般性的问题，应通过数据安全法解决。 **(b) 非强制性要求的适用** 此外，我们建议明确说明： • 处理活动仅需遵守相关法律法规的强制性要求；且 • 各个实体无需严格采用推荐性标准或最佳做法（这些标准或最佳做法应符合我们就第十一条所提出的建议中所提到的国际标准），但对于需遵循哪些标准或做法应有一定程度的自由裁量空间，以使这些实体能遵守个人信息保护法项下的强制性要求或选择在强制性要求以外做的更多。
11	We note that the State will establish a system for personal information protection. We add that the implementation of global standards and other systems is crucial to developing the PRC financial market and attracting foreign investors. This is particularly relevant to multinational financial institutions which typically use, process or store personal information in multiple locations. If the system is not compatible with international standards and other systems, it may result in conflicting legal and regulatory obligations, which will pose significant challenge to multinational financial institutions.	We make the following recommendations here: **(a) Adopting existing international standards and best practices** We are of the view that any system for personal information protection established by the State should recognise and adopt relevant international standards as much as possible. If full adoption is not possible, the system should be aligned with relevant international standards, and be formulated by having regard to overseas practices to ensure the efficient flow of personal information and compatibility in practice, particularly in the context of cross-border financial activities. **(b) Involving impacted foreign entities in the design process** Given that foreign entities will be materially impacted by the extra-territoriality of the PIPL, we recommend

Article 条款	Comments 意见	Recommendations 建议
		that the government establishes the system with participation on a voluntary basis by relevant stakeholders, including foreign entities, to ensure practicality and effectiveness.
第十一条	我们注意到，国家将建立个人信息保护制度。 此外，实施全球性的标准和其他制度，对发展中国金融市场和吸引外国投资者至关重要。这与跨国金融机构尤其相关，因为他们通常在多个地点使用、处理或存储个人信息。如果该制度与国际标准和其他制度互不兼容，则可能会导致法律和监管义务的冲突，这将对跨国金融机构构成重大挑战。	我们在此提出以下建议： **(a) 采用现有的国际标准和最佳做法** 我们认为，国家建立的任何个人信息保护制度都应尽可能地承认和采用相关的国际标准。如果无法完全采用，则该制度应与相关的国际标准具有相当一致性，且在制定时应考虑到境外的实践，以确保个人信息的高效流动及实践做法的兼容（尤其是在跨境金融活动的语境下）。 **(b) 让受影响外国实体参与设计过程** 鉴于外国实体将受到个人信息保护法的域外法权的重大影响，我们建议政府建立由利益相关者（包括外国实体）自愿参与的制度，以确保实用性和有效性。
12	We note that the State will participate in the formulation of international rules on personal information protection, promote international exchange and cooperation in the area of personal information protection, and promote the mutual recognition of personal information protection rules and standards with other countries, regions and international organisations.	We recommend that international standards with respect to cross-border transfers of personal information – such as the APEC Cross-Border Privacy Rules (“CBPR”) – are taken into account when designing the cross-border data controls to facilitate the secure flow of personal information under Chapter 3 and elsewhere in the PIPL.[6]
	我们注意到，国家将参与个人信息保护国际规则的制定，促进个人信息保护领域的国际交流与合作，并促进与其他国家、地区和国际组织之间相互认可个人信息保护规则和标准。	我们建议，在设计跨境数据控制时，应考虑到有关个人信息跨境提供的国际标准（例如亚太经合组织的跨境隐私规则（CBPR），以便促进个人信息保护法第三章和其他部分中所规定的个人信息的安全流动。

[6] For example, the Cross-Border Privacy Rules (CBPR) System developed by the Asia Pacific Economic Cooperation (APEC) forum: http://cbprs.org/.
例如，由亚太经济合作组织（APEC）论坛开发的跨境隐私规则（CBPR）系统：http://cbprs.org/。

Article 条款	Comments 意见	Recommendations 建议
Chapter II Rules on Processing of Personal Information **第二章 个人信息处理规则**		
13	We note that more grounds for collecting and processing personal information have been introduced under the PIPL. However, there is no provision equivalent to the ground under Article 6.1(f) of the GDPR in respect of "processing… necessary for the purposes of legitimate interests pursued by the controller or by a third party", although this has been introduced in a number of Asian data privacy regimes. We also note that only five out of the eleven exceptions to consent under the 2020 Specification have been included under the PIPL. In addition, more practical processing grounds are seen in the data protection regimes of other financial centres in Asia [7]. Although "legitimate interest" is not explicitly stated in the laws to those regimes, more specific grounds are provided to allow enterprises to carry out functions without causing disruption to normal and legitimate activities. Seeking individuals' consent can be impracticable and negatively impact activities in the finance service industry such as conducting risk assessments and combating financial crimes such as anti-money laundering (which relies heavily on public domain data (sanction lists, court decisions, bankruptcy information, etc.)). Separately, in the context of the collection and processing of personal information in an electronic form through a network, it is	We recommend that the PIPL avoid establishing consent (in any form) as the primary legal basis for collecting, using, disclosing or otherwise processing personal information including its cross-border transfer. Consent, as it is proposed in the PIPL, creates a degree of legal uncertainty as consent is always capable of being withdrawn. This uncertainty creates inherent operational and compliance issues which could be avoided if other legal grounds for processing are treated as equally legitimate alternatives to consent. For these reasons, we urge the Commission to adopt the concept of "legitimate interests" of the processor as an additional processing ground, which requires the processor to balance the risk associated with a particular processing activity with the rights and interests of the data subjects. As such, the Commission should reconsider how consent should work in practice and, indeed, whether it is necessary in light of the protections for individuals that already exist under various laws and regulations at national and industry levels.

[7] For example, the Singapore Personal Data Protection Act (Third Schedule, article 1(c)) permits the use of personal data about an individual without consent in various circumstances including where the personal data is publicly available. Likewise, under the Hong Kong Personal Data (Privacy) Ordinance, data collection and use for the function and activities of firms are generally permissible so long as notification is provided to data subjects (DPP1 Schedule 1 of the PDPO).

例如：新加坡《个人资料保护法》（附件三第 1(c)条）允许在包括关于个人的个人资料可以公开得到等各种情况下，可未经同意而使用该等个人资料。同样，在香港《个人资料（私隐）条例》下，只要数据主体获得告知，则为企业的职能及活动而收集及使用资料一般是允许的（《个人资料（私隐）条例》附表 1 中保障资料原则的第 1 原则）。

Article 条款	Comments 意见	Recommendations 建议
	unclear how the consent requirement in Articles 41 and 42 of the CSL would work in light of the processing grounds (other than consent) in Article 13 of the PIPL.	We recommend that, if the Commission believes that it is not appropriate to include a "legitimate interests" processing ground in the PIPL, the ground of "where processing is essential to maintaining safe and stable operation of a product or service" provided under the 2020 Specification should be included in the PIPL as an exception to obtaining consent. The Commission should also consider including in the PIPL other exceptions to consent from the 2020 Specification to maximise the practical efficiency of doing business. We suggest clarifying how the consent requirement/principle set out in Articles 41 and 42 of the CSL should be observed in light of the processing grounds (other than consent) in Article 13 of the PIPL. We also suggest clarifying "circumstances as may be provided by laws or administrative regulations" with a list or hyperlinks to appropriate laws, rules, and regulations to provide greater clarity. In addition, we suggest clarifying whether Article 13(3) of the PIPL includes fulfilment of duties, responsibilities or obligations under overseas laws and regulations. This is crucial in enabling international financial institutions to meet their compliance obligations (and such compliance is frequently monitored by the financial regulators in China).

Article 条款	Comments 意见	Recommendations 建议
第十三条	我们注意到个人信息保护法下为收集和处理个人信息引入了更多的依据。但是没有任何等同于 GDPR 第 6.1(f) 条的依据，即“为控制权人或第三方追求的合法利益而进行的对……必要的处理”，尽管亚洲的一些资料隐私制度中已经引入了这一点。 我们也注意到 2020 年规范下关于同意的 11 项除外项目中，只有 5 项已包括在个人信息保护法之中。此外，在亚洲其他金融中心的资料保护制度中体现了更为实际的处理依据[6]。尽管该等制度的法律没有明确说明“合法利益”，但规定了更具体的依据，让企业可以在没有对正常合法的活动造成干扰的情况下履行职能。寻求个人同意可能在实践中不具有可操作性，且对金融服务业进行例如风险评估及打击反洗钱（这很大程度上依赖公有领域的资料（制裁名单、法院判决、破产信息等））等金融犯罪等活动造成负面影响。 此外，在通过网络以电子方式收集和处理个人信息方面，不清楚根据个人信息保护法第十三条规定的处理依据（取得同意除外），网络安全法第四十一条和第四十二条规定的同意要求如何实行。	我们建议，个人信息保护法应避免将（任何形式的）同意作为收集、使用、披露或以其他方式处理个人信息（包括跨境转移）的主要法律依据。如个人信息保护法中所提议，同意会造成一定程度的法律上的不确定性，因为同意总是可以撤回的。这种不确定性将一定会带来运营和合规方面的问题，但如果将信息处理的其他法律依据视为可以取代同意的同等合法选择，则可以避免这些问题。鉴于这些理由，我们促请法工委采用处理者的“合法权益”概念作为额外的处理依据，这要求处理者在与特定处理活动相关的风险与数据主体的权益之间取得平衡。因此，法工委应重新考虑这一同意要求在实践中应如何发挥作用，以及在各部全国性和行业性的法律、法规下已对个人提供的保护的情况下，这一同意要求是否还有必要。 我们建议，如果法工委认为将“合法利益”作为处理依据纳入个人信息保护法中并不适当，应在个人信息保护法中纳入 2020 年规范下规定的“维护所提供产品或服务的安全稳定运行所必需的”，作为取得同意的豁免情况。法工委还应考虑将 2020 年规范规定的豁免同意的其他情况纳入个人信息保护法，将营商的实践效率最大化。 鉴于个人信息保护法第十三条所列的处理依据（取得同意除外），我们建议澄清应如何遵守网络安全法第四十一条和第四十二条所述的同意要求/原则。我们还建议对“法律、行政法规规定的其他情形”作出更清楚的说明，列明适当的法律、规则和法规或者加入该等法律、规则和法规的链接。 此外，我们还建议澄清个人信息保护法第十三条第（三）项是否包括海外法律法规下的职责、责任或义务。这对于国际金融机构履行其合规义务至关重要（中国的金融监管机构经常对这种合规性进行监督）。

Article 条款	Comments 意见	Recommendations 建议
14	We note that any consent for processing personal information must be given "explicitly" / "unambiguously", but this concept is not explained in any more detail. Although an "opt-out"-type of consent, or consent implied through action, is not expressly prohibited under the PIPL, it is not clear from the terms "explicitly" / "unambiguously" whether consent must be given expressly or by a positive act. This Article also introduces a concept of a "separate consent", which will need to be obtained from a data subject in respect of certain processing activities prescribed by law and regulations. In the PIPL, "separate consent" is also referred in Articles 14, 24, 26, 27, 30 and 39. However, there is no definition of, or further explanation how to legitimately obtain, "separate consent" under the PIPL. In addition, the Draft PIPL does not address (in Article 14 or elsewhere) situations where enterprises collect personal information indirectly, as is contemplated clearly under the 2020 Specification (Article 5.4(e)). This should be resolved in order to enable enterprises to collaborate for the sake of business efficiencies and in the interest of customers and employees. We note that, where there is a change in the "processing method" that a data subject has previously consented to, consent of the individual should be sought again. On the other hand, it should also be borne in mind that individual data subjects are not likely to wish to be constantly approached to provide separate consents each time, which may result in so-called "consent fatigue" – i.e. the individuals may not take time to understand the consent notifications and just accept and move on, which defeats the PIPL's objective of ensuring that	We recommend as follows so that financial institutions can better understand how to satisfy these fundamental requirements under the PIPL in practice: **(a) Meaning of "explicit" or "unambiguous" consent** We suggest clarifying the meaning of consent being given "explicitly" / "unambiguously". **(b) Meaning of "separate" consent** We suggest clarifying the meaning of "separate consent". **(c) Indirect collection of personal information** We suggest explaining explicitly the viability of consent being relied on by the personal information processor in the circumstance that personal information is obtained indirectly by the processor. This would accord with the requirements for indirect acquisition of personal information under Article 5.4(e) of the 2020 Specification. **(d) Renewed consent** What would constitute a "change" in the method of processing personal data that would require a financial institution to have to obtain a new consent seems difficult to assess i.e. whether all changes in method of processing should trigger this obligation. We suggest removing this concept from the PIPL or, if it must be retained, it will be important to clarify the meaning of "change in the method of processing personal data".

Article 条款	Comments 意见	Recommendations 建议
	individuals are ideally informed of the circumstances surrounding the collection and processing of their personal information.	
第十四条	我们注意到，任何处理个人信息的同意，必须“明确”作出意思表示，但条文中并未详细说明这一概念。虽然个人信息保护法并未明文禁止以“预设默许”的方式取得同意或以行动作为默示同意，但不清楚“明确”一词是否指必须明示同意或以主动作为给与同意。 本条还提出了“单独同意”的概念，即必须就法律和法规规定的若干处理活动取得数据主体单独同意。个人信息保护法第十四、二十四、二十六、二十七、三十和三十九条也提到“单独同意”，但个人信息保护法并未界定“单独同意”的含义，也未深入说明取得“单独同意”的合法途径。 此外，个人信息保护法草案并未（在第十四条或其他部分中）就企业间接收集个人信息的情况作出规定， 2020 年规范对此有清楚的规定（第 5.4(e)条）。这一点需要解决，以便企业能够彼此合作，既可提高经营效率，也符合客户和雇员的利益。 我们注意到，如果数据主体先前同意的“处理方式”发生变更，应当重新取得个人同意。 另一方面，应注意到，个人数据主体未必喜欢经常收到请其单独同意的请求，如每次均须数据主体单独同意，可能会造成所谓的“同意疲劳”，即个人未必会再花时间了解同意通知的内容，而只会干脆同意了事。这样一来便违背了个人信息保护法的原意，即要确保个人充分知悉与其个人信息的收集和处理相关的情形。	我们提出以下建议，使金融机构能够更好了解如何实际满足个人信息保护法的这些基本规定： **(a) “明确”同意的含义** 我们建议清楚说明“明确”同意的含义。 **(b) “单独”同意的含义** 我们建议清楚说明“单独同意”的含义。 **(c) 间接收集个人信息** 我们建议清楚说明如个人信息处理者间接获取个人信息，可以依赖已有同意的有效性。这一规定与 2020 年规范第 5.4(e)条关于间接获取个人信息的规定是一致的。 **(d) 重新取得同意** 哪些个人信息处理方式的“变更”需要金融机构重新取得个人同意这一点似乎难以判断，是否处理方式的所有变更均会触发这一义务？我们建议个人信息保护法删除这个概念，如果必须保留的话，清楚界定“个人信息的处理方式发生变更”的含义这一点很重要。

Article 条款	Comments 意见	Recommendations 建议
17	This article states that personal information processors may not refuse to provide products or services even if an individual does not consent to the processing of his/her personal information, except where the processing of personal information is necessary for the provision of products or services.	We recommend that the obligation to continue the provision of products or services under this article should only apply where the personal information that the organisation seeks to collect and process is not within the reasonable (objective) expectation of the individuals concerned. We submit that necessity is a high threshold and organisations will find this requirement challenging as there will be circumstances where it is reasonable to expect that personal information would be processed although it may not be strictly necessary to process personal data, for example, where an organisation wishes to engage vendors to process personal data.
第十七条	本条规定，即使个人不同意处理其个人信息，个人信息处理者也不得拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。	我们建议，只有当组织所寻求收集和处理的个人信息不在有关个人的合理（客观）期望范围内时，才应继续适用本条项下继续提供产品或服务的义务。 我们认为，必要性是一个很高的门槛，组织会发现这一要求具有挑战性，因为在某些情况下可以合理地预期将会处理个人信息，虽然可能并不一定非要处理个人数据，例如，在某一组织希望聘请供应商处理个人数据时。
19	The circumstances under which confidentiality must be preserved are unclear. For example, a standard confidentiality clause in a commercial contract would appear to trigger this exemption.	We recommend clarifying the confidentiality requirements contemplated by the article to allow financial institutions to comply in practice.
第十九条	不清楚在何种情形下应当保密。例如商业合同中的标准保密条款似乎已可触发这项豁免。	我们建议清楚说明本条关于保密的规定，使金融机构能够实际遵行。
22	The concepts of “personal information processor” seems well defined under the PIPL but the concept of an “entrusted party” is vaguer. Other international regimes, notably the GDPR, have specific definitions of “data controller” and	**(a) Differentiation of concepts of “controller” and “processor”**

Article 条款	Comments 意见	Recommendations 建议
	"data processor" to allow a clear designation of different rights and obligations in flows of personal information. Given the importance of service providers and other types of "entrusted party" in a vibrant digital ecosystem, the PIPL may benefit from similar specificity. As an example, we note that "controller" is defined clearly under the 2020 Specification (and its previous iteration) (Article 3.4) but a clear definition concept of "processor" is omitted. Although the PIPL sets out the obligations of an entrusted party which is entrusted to process personal information, it is unclear how liability arising from the infringement of a data subject's personal information rights should be allocated between the personal information processor and the entrusted party.	We recommend that clearer delineation is prescribed under the PIPL for the concepts of "data processor" and "entrusted party" (or alternative phrases such as "data controller" and "data processor" are adopted to align with the terminology of other international markets). **(b) Liability allocation** We suggest clarifying how an entrusted party will be liable to a data subject under the PIPL.
第二十二条	个人信息保护法对"个人信息处理者"的概念似乎有清晰的定义，但"受托方"这一概念的含义则较含糊。其他国际制度、特别是 GDPR，对"数据控制者"和"数据处理者"有具体的定义，以便清楚规定个人信息流动过程中各方的权利和义务。鉴于服务提供方和其他各类"受托方"在一个蓬勃的数字生态系统中起着重要作用，个人信息保护法也许适宜作出同样具体的规定。例如，我们注意到 2020 年规范（及其先前的版本）（第 3.4 条）对"控制者"有清楚的定义，但没有清楚界定"处理者"的概念。 尽管个人信息保护法对受托处理个人信息的受托方的义务作了规定，但不清楚个人信息处理者和受托方之间应如何分担因侵犯数据主体的个人信息权利而引致的责任。	**(a) 区分"控制者"和"处理者"的概念** 我们建议在个人信息保护法中更清晰地规定"数据处理者"和"受托方"的含义（或改用诸如"数据控制者"和"数据处理者"之类的术语，以便和其他国际市场的用语保持一致）。 **(b) 责任分担** 我们建议清楚说明受托方在个人信息保护法下将会如何对数据主体承担责任。
24	**(a) Separate consent for transfers to third parties** Separate consent is required from individuals where a personal information	**(a) Reduce (if not remove) separate consent requirements** We suggest specifying that the disclosure of personal information to

Article 条款	Comments 意见	Recommendations 建议
	processor engages a third party to process the personal information. However, in such circumstances, there may be other legal basis for processing personal information. Moreover, this requirement is not consistent with Article 13 as Article 13 provides other legal basis apart from consent for a processor to process personal information. Also, it seems impractical for the same requirements to apply to transfers of personal information within the same corporate group (including between different branches) as for transfers to third parties, in particular that separate consent should be required for affiliate transfers. **(b) Notification requirements** It would not be practicable to notify individuals of the identity of each of third-party recipient, the contact information of the third party, and the processing method, as required under this article. In addition, in business activities conducted between two entities, there could be cases where certain personal information is provided by one entity to the other. It would not be practical for the receiving entity to reach out to the individuals directly to obtain their consents to onward disclosure of the personal information to a third party. (c) The second paragraph of this article asserts that third parties may not use technical or other methods to reidentify individuals in anonymised information. However, pursuant to item 4 under Article 69, anonymised personal information is required to undergo processing to make it impossible to restore the identity of the individual. Therefore, this second paragraph would seem redundant.	third parties is permitted if any of the processing grounds established under Article 13 (other than the consent of the individual) is met. Also, we suggest expressly providing that where a processing ground applies pursuant to Article 13, the sharing, disclosure, and transfer of personal information: (1) within the same organisation or corporate group, including between and among different branches; and (2) with the organisation's third party vendors (for example, for the purposes of the performing or fulfilling of a contract with data subjects such as the organisation's clients or employees), should not require a "separate consent". **(b) Narrow notification requirements** We recommend that the categories of recipients be notified to individuals instead of the exact identities of the recipients. This is consistent with international norms, including GDPR (Article 13.1(e)). **(c) Indirect acquisition** We recommend clarifying that, for further disclosure of personal information disclosed by one entity to another entity, the receiving entity can rely on the consent provided by the disclosing entity to further disclose the personal information to any third parties (instead of requiring that the receiving entity obtains consent from the relevant individuals directly). This would accord with the requirements for indirect acquisition of personal information under Article 5.4(e) of the 2020 Specification. **(d) Anonymisation** In addition, we would recommend that the second paragraph of this article is omitted for the reasons cited.
第二十	**(a) 向第三方提供信息须取得单独同意**	**(a) 降低（若非删除）单独同意要求**

Article 条款	Comments 意见	Recommendations 建议
四条	个人信息处理者委托第三方处理个人信息须取得个人的单独同意。但是，在这种情形下，可能还有其他可处理个人信息的法律依据。并且该要求与第十三条的规定并不一致，因为第十三条提供了除个人同意之外的其他处理个人信息的法律依据。 此外，对于在同一公司集团内（包括不同分支机构之间）进行的个人信息传输适用与向第三方传输的同等要求，尤其是向关联方传输也需要单独同意，似乎是不切实际的。 **(b) 告知要求** 按照该条要求向个人告知每一第三方接收人的身份、联系方式以及处理方式是不切实际的。 此外，在两个实体之间进行的业务活动中可能会出现一方向另一方提供某些个人信息的情况。要求接收实体直接与个人联系以取得他们的同意将个人信息继续披露给第三方是不切实际的。 (c) 该条第二段规定第三方不得利用技术等手段对获提供的匿名化信息重新识别个人身份。但是，根据第六十九条第（四）项，个人信息匿名化须对个人信息经过处理使其无法复原识别个人的身份。因此，该第二段规定似显多余。	我们建议明确，如果第十三条规定的任何处理依据（除个人同意之外）得到满足，即可向第三方披露个人信息。 另外，我们建议明确规定，如第十三条规定的某一处理依据适用，则 (1) 在同一组织或公司集团内（包括在不同分支机构之间）共享、披露和传输个人信息；及 (2) 与该组织的第三方供应商共享、披露和传输个人信息（例如为履行一份与数据主体（如该组织的客户或员工）签订的合同之目的），均无需取得“单独同意”。 **(b) 降低告知要求** 我们建议向个人告知接收人所属类别，而非确切身份。这与国际规范一致，包括 GDPR（第 13.1(e)条）。 **(c) 间接获取** 我们建议明确，对于一个实体继续向其他实体披露个人信息的情况而言，接收实体可以依赖披露实体提供的同意进一步向任何第三方披露个人信息（而无需接收实体直接向相关个人获取同意）。这符合 2020 年规范第 5.4(e)条关于间接获取个人信息的要求。 **(d) 匿名化** 此外，我们建议删除本条的第二段，原因如前所述。
25	There is no threshold or other guidance as to when guarantees of transparency, fairness and reasonability are triggered when personal data is used in automated decision making (“**ADM**”). While it can be argued that the principles of processing (e.g. Article 7 in respect of openness and transparency) can be said to apply generally to all forms of processing, Article 25 is specific in that it requires “reasonability of the handling result” to be guaranteed. This is problematic owing to	We recommend that such guarantees be provided only if use of ADM “produces legal effects concerning him or her or similarly significantly affects him or her” and where solely ADM is used. For the obligation to explain to not be subject to ADM processing, we recommend clarifying what would constitute “material influence in their rights and interests”. Further, we propose to include

Article 条款	Comments 意见	Recommendations 建议
	the black-box uncertainty and "un-explainability" that is inherent some AI algorithms we see today. This article further introduces an obligation to explain, and for data subjects to not be subject to, ADM processing if there is a "material influence in their rights and interests".	exceptions to such obligation where (i) an individual's consent has been obtained, or (ii) it is necessary for performance of the relevant contract to do so; or (iii) otherwise lawful to do so. These proposals are consistent with international norms, including the GDPR (Article 22).
第二十五条	对于在利用个人信息进行自动化决策时（"**自动化决策**"）何时会触发有关透明度及公平合理的保证，并无标准或其他指引。尽管可以认为处理原则（例如第七条关于公开、透明的原则要求）普遍适用于所有形式的处理，但第二十五条具体要求"处理结果的公平合理" 得到保证。由于存在黑匣子不确定性以及我们今天看到的某些人工智能算法固有的"不可解释性"，该等会要求存在一定问题。 该条进一步规定了数据主体在"对其权益造成重大影响"的情况下有权要求说明以及拒绝通过自动化决策作出决定相关的义务。	我们建议仅在使用自动化决策会"对其产生法律效力或类似的重大影响"以及仅通过自动化决策的情况下提供该等保证。 关于与要求说明以及拒绝通过自动化决策作出决定相关的义务，我们建议明确什么会构成"对其权益造成重大影响"。 另外，我们建议对该等义务规定例外情形，包括（i）已取得个人同意，或（ii）为履行相关合同所必需；或（iii）其他依法进行的情形。 这些建议与国际规范一致，包括 GDPR（第 22 条）。
26	It is unclear what is concept of "publishing" under this Article is intended to entail. This Article addresses separate consent for the publication of personal information.	We recommend clarifying the concept of "publish" under this Article, which may similarly to the 2020 Specification include an exception for disclosures by the personal information processor to an affiliated entity. If an organisation is beholden to a "just in time" consent requirement, this article could create an operational challenge and we recommend consent be obtained at the point of collection *or* disclosure. Repository maintenance of multiple consents will create additional concerns.
第二十六条	该条所述的"公开"意在包括哪些情形并不明确。 该条是针对公开个人信息的单独同意。	我们建议明确该条中"公开"的含义，与 2020 年规范类似，可将个人信息处理者向关联实体披露排除在外。 如果某个组织须遵守"即时"同意要求，则该条规定可能会带来操作上的困

Article 条款	Comments 意见	Recommendations 建议
		难。我们建议在收集*或*披露时获取同意。多个同意的存储维护会产生其他问题。
28	We note that the PIPL imposes additional obligations on disclosure of personal information. Separate consent is necessary where the processing cannot be conducted within a reasonable scope related to the purpose for which the information was originally disclosed or, if such purpose is unknown, to use the information would have a material impact on the data subject. However, with many financial services firms increasingly deploying automated software and other tools to collect and process personal information from the public domain in order to enhance business efficiency (e.g. supporting risk assessment business and for combatting financial crime through AML/KYC processes, which rely heavily on public domain data including sanction lists, court decisions, bankruptcy information, etc.), especially with use of such technological tools being promoted by the People's Bank of China's Fintech Development Plan for 2019-2021, it would be difficult for financial institutions to contact and obtain consent from all customers and prospective customers for these purposes. In addition, it is unclear what is the meaning of "reasonable scope" under which no consent is required from the relevant individuals.	We suggest that the PIPL could refer to the 2020 Specification whereby automated software and similar techniques can be adopted to collect and process personal information in the public domain without the need for the data subject's consent. We suggest clarifying the meaning of definition of "reasonable scope", e.g. by explicit cross-reference to Article 7.3(a) of the 2020 Specification if applicable.
第二十八条	我们注意到个人信息保护法对个人信息的披露规定了更多义务。如果处理个人信息超出与该个人信息被公开时的用途相关的合理范围，或被公开时的用途不明确而使用该个人信息会对数据主体有重大影响，则须取得单独同意。 但是，随着许多金融服务公司为提高业务效率越来越多地采用自动化软件和其他工具来收集和处理来自公共领域的个人信息	我们建议个人信息保护法可参照 2020 年规范，允许采用自动化软件和类似技术来收集和处理公共领域的个人信息，而无需征得数据主体的同意。 我们建议明确"合理范围"的定义，例如通过明确提述 2020 年规范第 7.3(a)条（如适用）。

Article 条款	Comments 意见	Recommendations 建议
	（例如，通过反洗钱 / “客户尽职调查”程序辅助风险评估业务及打击金融犯罪，而这类程序极大地依赖于包括制裁清单、法院裁决、破产信息等在内的公共领域信息），尤其是在中国人民银行发布的《金融科技发展规划（2019-2021 年）》推广使用此类技术工具的背景下，金融机构很难为此目的联系所有客户和潜在客户取得其关于该等使用目的的同意。 另外，无需相关个人同意的“合理范围”的含义并不清楚。	
Chapter III Rules on Cross-Border Provision of Personal Information **第三章 个人信息跨境提供的规则**		
29	The definition of “sensitive personal information” is different from that under the 2020 Specification.	We recommend clarifying which definition of “sensitive personal information” should be followed and being consistent across different rules and guidelines to assist ease of compliance.
第二十九条	“敏感个人信息”的定义与 2020 年规范下的定义有所不同。	我们建议澄清“敏感个人信息”所应适用的定义，并且为便于遵守，建议在不同的规定和指引中保持该等定义的统一。
30	This article requires separate consent for the processing of sensitive personal information. In business activities conducted between two entities, there could be cases where certain personal information is provided by one entity to the other. It would not be practical for the receiving entity to reach out to the individuals directly to obtain their consents to process the relevant personal information.	As for Article 26, if an organisation is beholden to a “just in time” consent requirement, this article could create an operational challenge and we recommend consent be obtained at the point of collection *or* disclosure. Repository maintenance of multiple consents will create additional concerns. We propose to include clarification that, for processing of personal information disclosed by one entity to another entity, the receiving entity can rely on the consent provided by the disclosing entity to process the sensitive personal information (instead of requiring the receiving entity to obtain consent from individuals directly). This would accord with the requirements for indirect acquisition of personal information under

Article 条款	Comments 意见	Recommendations 建议
		Article 5.4(e) of the 2020 Specification. We would also urge an exception is provided where processing sensitive personal information is required by law and to protect vital interests.
第三十条	根据该条规定，处理敏感个人信息时，必须取得单独同意。 在两个实体之间进行的业务活动中，一个实体可能向另一家实体提供某些个人信息。处理相关个人信息时，接收该等个人信息的以方在实践中往往不便直接征求个人同意。	如一个组织因第二十六条的规定而受限于“及时”同意的要求，则该条款可能存在实操的问题。我们因此建议在收集或披露信息时，征求同意。对多项同意的数据库维护也将产生额外问题。 我们建议澄清，对于处理一家实体向另一家实体披露的个人信息，接收方可依赖披露方提供的同意处理敏感个人信息（而非要求接收方直接向个人征求同意）。这符合 2020 年规范第 5.4(e)条关于间接获取个人信息的要求。 我们还促请，对相关法律要求处理敏感个人信息和保护重大利益的情况，作出除外规定。
38 第三十八条	**(a) Lack of clarity on security assessment and certification requirements** It is unclear whether the security assessment under item 1 of Article 38 and the certification under item 2 of Article 38 constitute one-time processes for each transfer, or if they cover repeated transfers of a similar nature. The scope of the assessment and the certification are also uncertain. In particular, we are concerned that requiring assessments/ certifications for each and every transfer are disruptive to business. Cross-border transfers within financial services groups are too frequent in the modern world of finance. In addition, the identity of the “professional agencies” and the scope of their responsibilities in the certification processes is unclear.	We propose clarifying the specific requirements for completion and frequency of these security assessment and certification obligations. For example, the 2017 Cross-Border Transfer Guidelines began to provide a level of detail that was more illustrative for business operations. Similarly, under Article 3 of the draft Measures on Security Assessment of Cross-border Transfer of Personal Information released in June 2019 (the “**2019 Draft Assessment Measures**”), cross-border transfers of personal information did not require further assessment for a period of two years unless the purpose, categories or overseas storage periods of relevant information were changed. If a security assessment or certification requirement is to remain, we would urge an exception for intra-group transfers to facilitate efficient business operation. See our similar comments in respect of Article 24.

Article 条款	Comments 意见	Recommendations 建议
		In addition, we recommend that more detail is provided on the identity, location (onshore or offshore) and the scope of responsibility of the professional agencies involved in the certification processes in order to ensure that there is transparency and accountability for financial institutions which are the subject of the processes.
	(a)安全评估和认证要求不明确 尚不清楚第三十八条第（一）项项下的安全评估和第三十八条第（二）项项下的认证是否适用于每一次信息转移，或多次类似性质的信息转移是否仅须进行一次此类安全评估和认证。评估和认证范围也尚不明确。尤其是，鉴于在现代金融世界，金融服务集团内部的信息跨境转移十分频繁，我们担心，若每次信息转移均要求评估/认证，业务运营将受到影响。 此外，“专业机构”的身份和其在认证流程中的责任范围也尚不清楚。	我们建议澄清有关完成该等安全评估和认证的具体要求和频率。比如，2017 年数据出境安全评估指南开始提供对业务运营更具说明性的具体规定。类似地，根据 2019 年 6 月颁布的《个人信息出境安全评估办法》（草案）（“**2019 年评估办法草案**”）第三条，两年内的个人信息的跨境出境不需要进一步评估，除非相关信息出境目的、类型和境外保存时间发生变化。 如果保留安全评估或认证要求，我们促请对集团内部转移作出除外规定，以促进高效的业务运营。请参见我们对第二十四条提出的类似意见。 此外，我们建议，对参与认证流程的转移机构的身份、所在地（境内或境外）和责任范围，作出更具体的规定，以确保对于作为流程当事人的金融机构的透明度和问责制。
	(b) High level requirements on contracts between personal information processors and foreign recipients. Item 3 of Article 38 provides an option for a personal information processor to transfer personal information outside of the PRC by concluding a contract with the foreign recipient. However, the PIPL does not provide any details on the necessary contractual terms.	We suggest that if any contractual terms are mandatorily required, in order to allow financial institutions to understand their obligations in practice, including in respect of onward transfers from the first overseas recipient, any implementing regulations or guidance should clarify that enterprises can rely on contractual terms that conform to international standards.

Article 条款	Comments 意见	Recommendations 建议
	(b) 对于个人信息处理者与境外接收者之间合同的严格要求 根据第三十八条第（三）项，个人信息处理者可通过与境外接收方订立合同的方式，向中国境外转移个人信息。但是，个人信息保护法并未就必要的合同条款作出具体规定。	我们建议，如强制要求载明任何合同条款，则为便于金融机构理解他们在实践中的义务，包括有关从前一家境外接收方的后续转移义务，任何实施细则或指引应明确企业可依赖符合国际标准的合同条款。
	(c) Affiliate exemption We note that “third parties” is very broad and would arguably include affiliated persons.	We suggest expressly providing that the sharing, disclosure and transfer of data within the same corporate group (including between different branches) should not be subject to any security assessment from the PIPL.
	(c) 关联方豁免 我们注意到，“第三方”的范围十分宽泛，可能包括关联人士。	我们建议明确规定，如在同一公司集团内（包括在不同分支机构之间）共享、披露和传输个人信息无需进行个人信息保护法下的任何安全评估。
	(d) Other exemptions In digital economies where transnational business promotes trade and improved service offerings, other markets provide other transfer mechanisms to facilitate legal and secure cross-border transfers of personal information. The options available under the PIPL are arguably lacking diversity to promote efficient business operations for the benefit of individuals within the PRC.	We recommend that other options to facilitate overseas transfer (without separate consent – see our comments on Article 39 below) should be included. Options to be considered include binding corporate rules, model contracts and certification schemes including the APEC CBPR as noted in our comments to Article 12.
	(d) 其他豁免 在跨境业务促进贸易和改善服务供给的数字经济中，其他市场存在其他转移机制，以便个人信息合法且安全地出境。个人信息保护法下的选择可能缺乏多样性，无法促进以中国境内个人利益为导向的高效的业务运营。	我们建议纳入其他便于信息跨境传输的选择（无需单独征求同意 – 见下文我们对第三十九条提出的意见）。其他选择包括具有约束力的公司规则、合同模板和认证机制，包括我们在上文对第十二条提出的意见中的 APEC CBPR。

Article 条款	Comments 意见	Recommendations 建议
39	If the personal information of a data subject will be transferred outside the PRC, the personal information processor must notify the individual of the identity and contact details (among other things) of the data recipient and a "separate consent" should be obtained from the individual. Notifying individuals of the identity of the exact recipient of the personal information is not practical for business. For multi-national companies, the list of recipients is often extensive. In addition, the list of recipients may change from time to time due to business needs. In addition, similar to our comments on Article 14, requiring individual's consent for every situation will place unnecessary burden on the individual and may result in "consent fatigue" without furthering the individual's privacy rights. Clients of the financial institutions will comprise institutional clients rather than individuals, so it is technically not the counterparties' consent that is required to collect and process any personal information, for instance for anti-money laundering / know-your-customer purposes (e.g. the information of the legal representative, directors, etc.). Market practice is that financial institutions in the PRC will seek contractual confirmations from the institutional client that it has first obtained consent from its representatives to provide their data to the financial institution as it is impractical for the financial institution to obtain each data subject's express written consent in this scenario. This accords with the requirements for indirect acquisition of personal information under Article 5.4(e) of the 2020 Specification.	**(a) Notification and consent requirements** Please see our comments on Article 14 in respect of the vagueness of the concept of "separate consent" and clarifying the meaning of "separate consent". Please also see our comments on Article 24 in respect of the recommendation that: (1) no separate consent should be required for the transfer of personal information within the same organisation or corporate group (including between different branches), and for transfers to third party vendors, where a processing ground under Article 13 already applies; and (2) that only the categories/types of third-party recipients should be notified to individuals. We would strongly recommend that the Commission considers that it would otherwise be difficult and impracticable in practice for financial institutions to satisfy this obligation if it requires enterprises to inform data subjects of the specific identity and contact details of each data recipient in advance of the transfer, rather than just the *categories/types* of third party recipients. The interests of data subjects ought to be assessed and balanced against the practical difficulties in the circumstances, especially where transfers are just to intra-group affiliates. We recommend combining Articles 38 and 39, such that transfers of personal information to parties outside the PRC is permitted if ***any one*** of the following conditions in Articles 38 and 39 are met. Please see our recommendations on Article 38 above. We also recommend specifying whether the indirect acquisition of personal information is recognised under the requirements of the PIPL. **(b) Local copy requirement**

Article 条款	Comments 意见	Recommendations 建议
		We suggest clarifying whether retaining a local copy of the personal information transferred overseas is also generally required.
第三十九条	如果数据主体的个人信息从中国向境外转移，个人信息处理者必须向该个人告知数据接收者的身份和联系信息（及其他相关信息），并应当向该个人“征求单独同意”。 对于企业而言，向个人告知个人信息接收者的身份并不实际。对于跨国公司，接收者很多。此外，接收者清单也会因为业务需要，不时发生变化。此外，与我们对第十四条提出的意见类似，每次均必须征求个人同意将导致个人承担不必要的负担，并可能导致“同意疲劳”，且不利于保护个人隐私权。 金融机构的客户是机构客户，而非个人，因此，在技术上，收集和处理任何个人信息时，必须征求的不是交易对手方的同意，比如出于反洗钱/了解您的客户的目的（比如法定代表人、董事等的信息），收集和处理任何个人信息。根据市场惯例，中国的金融机构必须要求机构客户订立合同，以确认其已取得其代表同意，可以向金融机构提供他们的信息，因为在该等情况下，金融机构不可能向每一数据主体征求明确书面同意。这符合 2020 年规范第 5.4(e)条关于间接获取个人信息的要求。	**(a) 通知和同意要求** 请参见我们对第十四条提出的意见，即有关“单独同意”概念模糊的意见和澄清“单独同意”的含义。请同时参见我们对第二十四条提出的意见，即建议（1）对同一组织或公司集团内（包括在不同分支机构之间）的个人信息转移及向第三方卖方的个人信息转移，在适用第十三条规定的处理事由的情况下，无需取得单独同意；以及（2）仅向个人告知第三方接收者所属范畴/类别。 我们强烈建议法工委考虑，对于金融机构而言，如果要求企业在转移前，向数据主体告知每一数据接收者的特定身份和联系信息，而非第三方接收者的所属范畴/类别，是困难且不切实际的。在该等情况下，必须根据实际问题，评估和平衡数据主体的利益，尤其是若仅向集团内部关联方转移。 我们建议合并第三十八条和第三十九条，在满足第三十八条和第三十九条中***任何一项***条件时，即可向中国境外转移个人信息。请见上文就第三十八条提出的建议。 我们还建议，说明个人信息保护法是否承认间接获取个人信息。 **(b) 当地副本要求** 我们建议澄清，是否普遍要求在当地留存出境个人信息的副本。
40 第四十条	**(a) Reconsideration of the localisation requirement** We assert that the proposed requirements around data localisation in Article 40 should be reconsidered, as	We strongly suggest removing the requirement to store personal information only in the PRC. Instead, new arrangements should be established to provide adequate protection to the data transferred

Article 条款	Comments 意见	Recommendations 建议
	localisation of personal information does not serve effectively to improve protection of individuals' rights and interests. In contrast, requirements mandating personal information to be retained onshore or be subjected to administrative procedures before transfers can be made are counterproductive. Localisation requirements give rise to many disadvantages including curtailing the financial industry's growth and compromising the effectiveness of cybersecurity and risk management controls. The restrictions serve to reduce product and service offerings, and impair the quality of any offerings, to Chinese clients, and ultimately negatively impact China's role and participation in international trade flows. Also, there are legitimate reasons for storing personal information outside the PRC, which we do not believe compromise national security or individual's rights. For example, multinational organisations may need to transfer aspects of employee personal information to head office to facilitate effective human resource planning and management. It is not practical to restrict the storage of personal information to the PRC in such circumstances.	offshore. Alternatively, if a localisation requirement must be retained, we suggest at least removing the requirement for security assessments to be completed by the State cyberspace authorities before financial institutions can transfer personal information outside of the PRC if they handle personal information above a certain threshold. This type of assessment on the basis of quantum of personal information involved is not in line with international norms.
	(a) 重新考虑本地化要求 我们主张重新考虑第四十条中拟规定的数据本地化要求，因为个人信息本地化无法有效改善个人权益的保护。相反，强制要求将个人信息保存在境内或者在转移前办理行政手续将产生相反效果。本地化要求会产生诸多弊端，包括阻碍金融业发展以及有损网络安全和风险管理控制的效果。该等限制性规定将降低向中国客户提供的产品和服务的数量与质量，最终对中国在国际贸易流中的作用和参与度产生负面影响。 同时，在中国境外存储个人信息存在合法理由，我们认为这样做并不有损于国家安	我们强烈建议删除仅在中国境内存储个人信息的要求。与此相反，应作出新的安排以对向境外转移的数据提供充分保护。 或者，如果必须保留本地化要求，我们建议至少删除若金融机构处理的个人信息超过特定门槛，则向中国境外转移个人信息前须通过国家网信部门安全评估的要求。这类基于所涉个人信息数量的评估不符合国际规范。

Article 条款	Comments 意见	Recommendations 建议
	全或个人权利。例如，跨国组织可能需要向总部转移员工个人信息以协助有效的人力资源规划和管理。在上述情况下将个人信息的存储位置仅限制在中国不切实际。	
	(b) Lack of definition of critical information infrastructure ("CII") operator The PIPL does not contain a definition of a CII operator. 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 PIPL and, if so, when the relevant provisions of the draft rules will be settled.	We suggest clarifying the definition of "CII" operator under the PIPL or expressly specify that CII operator should have same meaning as that under the CSL, and providing a definitive timetable for release 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 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 56.
	(b) 缺少关键信息基础设施运营者的定义 个人信息保护法未规定关键信息基础设施运营者的定义。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**"）拟采用两项标准测试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，金融机构无法确信个人信息保护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敲定。	我们建议，明确个人信息保护法下的关键信息基础设施运营者的定义或者明确规定，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规定存在歧义的其他条例明确的颁布时间表。 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五十六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。

Article 条款	Comments 意见	Recommendations 建议
	(c) Clarity is needed on the interpretation of "personal data collected or generated inside China" It is not entirely clear if "personal data collected or generated inside China" also covers foreign data (e.g. relating to foreign individuals) that is transferred into mainland China and processed locally for some reason.	Following from our comments on Article 3, we suggest clarifying the scope of "personal data collected or generated inside China". In particular, the 2017 Cross-Border Transfer Guidelines stated that, if the data is generated or collected offshore, transferred to the PRC, and subsequently transferred offshore without any alteration in the PRC, such data transfer would not be subject to the requirements on data transfer. We suggest that this principle be incorporated into the PIPL.
	(c) 需要明确解释何为"在中国境内收集或产生的个人信息" 尚不完全清楚"在中国境内收集或产生的个人信息"是否涵盖因某种原因转移至中国大陆并在当地处理的外国数据（例如，外国个人的相关数据）。	上接我们对第三条提出的意见，我们建议明确"在中国境内收集或产生的个人信息"的范围。特别是 2017 年数据出境安全评估指南规定，若境外产生或收集的数据转移至中国境内且在中国境内未作任何改变，之后再转移至境外，则该等数据转移不受限于数据转移要求。我们建议将该原则纳入个人信息保护法。
	(d) Exceptions for the cross-border data transfer The application of Article 40 is extremely broad. We submit that the localisation requirements (if they apply at all) should not apply to cross-border transfers of personal information between intra-group companies and to business or commercial relationships.	We would urge exceptions for intra-group transfers and transfers under business or commercial relationships to facilitate efficient business operation.
	(d) 跨境数据转移的例外情形 第四十条的适用范围非常宽泛。我们认为，本地化要求（若适用）不应适用于集团内部成员公司之间的个人信息跨境转移以及向具有业务或商业关系的主体跨境转移个人信息。	我们促请将集团内部转移以及业务或商业关系中的转移规定为例外情形，以便促进业务的高效运营。
41	We refer to Article 177 of the Securities Law which restricts the disclosure of securities business-related data to overseas regulators.	**(a) Conflict with foreign regimes** We recommend expressly clarifying that this Article does not apply:

Article 条款	Comments 意见	Recommendations 建议
	We understand that the existing position is now proposed to be expanded in respect of personal information stored within the PRC that may be requested by foreign law enforcement bodies, similar to the obligation in respect of data under Article 33 of the DSL. 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 disclosure, then the financial institutions may be in breach of the law of the other jurisdiction.	(a) to personal information that is not likely to endanger national security or public interest. Types of data which could have such an impact should be expressly dealt with under the DSL or any related rules or regulations; (b) to personal information stored in the PRC merely by virtue of its storage in a cloud server located in the PRC; (c) when the export of personal information is to facilitate intra-group assessment or reporting for anti-money laundering and counter-terrorism financing purposes; (d) to provision of personal information to international organisations (e.g. Interpol); or (e) to provision of personal information to foreign government authorities as required by the applicable local laws. 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, and the China Bank and Insurance Regulatory Commission's restriction on the transmission of client data to an offshore vendor regardless of whether the data is encrypted). **(b) Discretion to determine obligations under international treaties** We suggest clarifying the intention of second paragraph of Article 41 in respect of which party is authorised to make the relevant decision. **(c) Clarification on the receiving party** We suggest clarifying that Article 41 only applies when the receiving party is an overseas regulator or similar body.

Article 条款	Comments 意见	Recommendations 建议
第四十一条	据我们所知，《证券法》第一百七十七条限制向境外监管机构披露与证券业务活动有关的数据。 我们了解到，目前的情况是，与数据安全法第 33 条规定的数据相关义务类似，有人建议将有关范围扩大至境外执法机构要求提供的在中国存储的个人信息。 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，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披露，有关金融机构可能会违反其他司法管辖区的法律。	**(a) 与外国制度相冲突** 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个人信息。数据安全法或任何相关法规或规章应明确规范可能产生该等影响的数据类型； (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个人信息； (c) 个人信息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； (d) 向国际组织（如国际刑警组织）提供个人信息；或 (e) 按照适用的当地法律要求向境外政府机构提供个人信息。 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））。 **(b) 自行决定国际条约项下的义务** 我们建议就哪一主体被授权作出相关决定阐明第四十一条第二款的意图。 **(c) 明确接收方** 我们建议明确第四十一条仅适用于接收方为境外监管机构或类似机构的情形。
42	One key concern on this Article is its extra-territoriality which we believe should be limited to the maximum extent possible in respect of supervising harm to the “the national security or public interest of the People’s Republic of China”. This overlaps with the powers provided under the DSL, which is the better law to deal	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 personal information processing outside of the PRC. Overlaps with any existing

Article 条款	Comments 意见	Recommendations 建议
	with matters of national security or public interest. In addition, similar to our comments made separately in our submission in respect of the DSL, the drafting of this Article may indicate some extra-territorial jurisdiction over non-PRC processing activities (e.g. to investigate whether they are harmful to the PRC's national security). We submit that the current drafting is too vague, and Article 42 could be interpreted in ways which result in conflicting legal obligations with respect to non-PRC processing activities for financial institutions. This has caused serious concerns amongst international financial institutions. The article also elaborates on sanctions under the DSL by stating that the CAC may include foreign organisations and individuals on a blacklist, limiting or prohibiting the provision of personal information to them under certain circumstances.	law should be minimised. We urge that the PIPL focuses on PRC processing activities, and any investigation or enforcement powers should not cover non-PRC processing activities: • the question of whether non-PRC processing 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 processing activities cause subsequent *unintentional* harm to national security or public interest, there may be an inadvertent result of finding a breach of the PIPL 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 processing activities outside of the PRC in order to be subject to any investigation or enforcement. In respect of the introduction of a CAC blacklist, we suggest clarifying on the scope and enforcement practices in relation to this list, for example identifying how onshore persons will be absolved of potential liability where they breach contractual obligations to provide personal information overseas.
第四十二条	本条我们关心的主要问题是域外法权，我们认为就监控危害“中华人民共和国国家安全、公共利益”而言，应尽可能限制域外法权的范围。该规定与数据安全法规定的权力相重叠，后者更适合规范国家安全或公共利益事项。 此外，与我们就数据安全法另行出具的意见相类似，本条的草案内容可能包含对中	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个人信息处理活动，尽可能避免个人信息保护法与现行法律重叠。 我们促请个人信息保护法应围绕中国境

Article 条款	Comments 意见	Recommendations 建议
	国境外信息处理活动的某种域外司法管辖权（如调查有关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，第四十二条可以不同方式解读，导致境外金融机构开展中国境外信息处理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。 本条还进一步细化了数据安全法规定的制裁措施，规定国信办可将境外组织和个人列入黑名单，在特定情况下限制或者禁止向其提供个人信息。	内个人信息处理活动制定，有关调查权或执法权不应覆盖中国境外的个人信息处理活动，理由如下： • 就中国境外个人信息处理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 • 如果某些中国境外个人信息处理活动在进行之后*并非故意*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个人信息保护法（无犯罪意图）。 我们建议调整标准，有害的中国境外个人信息处理活动需要至少有一定程度的主观故意，方可展开调查或执法。 关于引入国信办黑名单，我们建议明确该清单的相关范围和执法行动，例如，明确境内人士违反向境外提供个人信息的合同义务时，将如何免除其潜在责任。
43	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 to which this Article 43 may apply.
第四十三条	不适用	我们建议明确以下事项： (a) 哪些措施构成"歧视性的禁止、限制或者其他类似措施"；

Article 条款	Comments 意见	Recommendations 建议
		(b) 私营实体即使注册成立于受质疑国家，仍不会受影响； (c) 负责监督所采取措施是否合法的相关机构；及 (d) 本第 43 条所适用的具体情形。
Chapter IV Rights of Individuals in Processing of Personal Information **第四章 个人在个人信息处理活动中的权利**		
Chapter IV in general	The draft law does not provide for limitations to individual rights prescribed in Chapter 4, Articles 44 to 49. Limitations to individuals' rights may be necessary, for reasons such as (but not limited to) protecting public interests, protecting the rights of other individuals and other legitimate reasons. Article 49 specifies that reasons must be provided to the individual if his or her request is rejected, which suggests an allowance for rejection of such rights. However, the lack of clarity in this article may result in challenges as to how it is implemented.	We recommend including a list of situations exempting organisations from responding to individuals' rights requests, such as conducting internal investigations, suspected malicious intent on the part of the requester, or due to the litigation proceedings. Similar and more expansive exemptions are provided in Article 8.7 of the 2020 Specification, which should be consistent with the principles in any revised version of these exceptions to the individuals' rights set out under the PIPL.
第四章整体	法律草案没有对第四章第四十四至第四十九条规定的个人权利作出限制。 出于（例如但不限于）保护公共利益，保护他人权利及其他合法原因，可能有必要对个人权利作出限制。 第四十九条规定拒绝个人行使权利的请求应当说明理由。这也表明在某些情况下可以拒绝个人行使权利的请求。但是，该条规定并不清楚，可能在实践中产生困难。	我们建议列明组织可免于响应个人行使权利请求的各项情形，例如进行内部调查，请求人可能存有恶意，或由于诉讼程序。2020 年规范第 8.7 条规定了类似而且更广泛的豁免，应与个人信息保护法下修改后的个人权利例外情形在原则上保持一致。

Article 条款	Comments 意见	Recommendations 建议
47	**(a) Conflict between Article 13 and Article 47** Where a financial institution processes personal information pursuant to its legal and regulatory obligations (such as for know-your-customer or regulatory reporting purposes) under Article 13(3) of the PIPL, it is unclear whether such financial institution must delete the personal information according to Article 47(3) of the PIPL if the relevant individuals withdraw their consents. **(b) Lack of clarification on technical difficulties** The article identifies that when technical difficulties are encountered in personal information processing and deletion of personal information, personal information processors must cease processing the personal information.	**(a) Clarification on Article 47(3)** We recommend clarifying that only when the processors process the personal information based on the consent of relevant individual, the relevant personal information should be deleted if such individual withdraws his or her consent. **(b) Clarification on technical difficulties** We recommend further clarifying what may constitute technical difficulty in this respect (examples or scenarios being welcomed).
47	**(a) 第十三条与第四十七条之间的冲突** 如果金融机构根据其在个人信息保护法第十三条第（三）项下的法定和监管义务（例如出于客户尽职调查或监管报告目的）处理个人信息，则在相关个人撤回同意的情况下，不清楚该等金融机构是否必须根据个人信息保护法第四十七条第（三）项的规定删除个人信息。 **(b) 技术困难不明确** 该条规定，如处理和删除个人信息从技术上难以实现，个人信息处理者应当停止处理个人信息。	**(a) 明确第四十七条第（三）项** 我们建议明确，只有在处理者基于个人的同意处理个人信息的情况下，才须在相关个人撤回其同意时有义务删除相关个人信息。 **(b) 明确技术困难** 我们建议进一步明确何种情形构成此处规定的技术困难（如有示例或情景说明更好）。
Chapter V Obligations of Personal Information Processors **第五章 个人信息处理者的义务**		
50	We submit that it is unclear under item (3) of Article 50 whether (i) it would be sufficient for an enterprise to adopt industry best practice for encryption and de-identification algorithms or (ii) it is required to adopt Chinese-formulated encryption algorithms.	We suggest clarifying the requirements on the encryption and de-identification algorithms so that the financial institutions know how to comply with this aspect under the PIPL.

Article 条款	Comments 意见	Recommendations 建议
	In addition, any overlap between this Article and Article 25 of the DSL and Article 11.1 of the 2020 Specification should be resolved.	More generally, similar requirements under the PIPL, DSL and 2020 Specification for appointment of a data protection officer should be reconciled.
50	我们认为，根据第五十条第（三）项，不太明确的是：（i）企业采用行业最佳做法进行加密和去标识化是否足够，或者（ii）必须采用中国制定的加密算法。 此外，应解决该条与数据安全法第 25 条和 2020 年规范第 11.1 条之间的重叠。	我们建议明确有关加密和去标识化算法的要求，以便金融机构清楚如何遵守个人信息保护法的这方面规定。 更宽泛而言，个人信息保护法、数据安全法和 2020 年规范中有关指定信息保护负责人的类似规定应相互协调一致。
51	**(a) Lack of specified threshold above which to appoint a person in charge of personal information protection** This Article requires that personal information processors who process personal information up to the quantities specified by the CAC must appoint a person in charge of personal information protection. However, the threshold amount has not been specified.	We suggest clarifying the specific threshold amount to be issued by the CAC prior to or at the time of promulgation of PIPL. The CAC may refer to the 2020 Specification which sets out specific numbers of employees and data subjects above which a person in charge of personal information protection is recommended to be appointed. It would be recommended that the mandatory threshold is higher than the "best practice" position.
	(a) 未明确须指定个人信息保护负责人的数量门槛 该条要求处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，但并未明确数量门槛。	我们建议在发布个人信息保护法之前或之时，对于将由国信办发布的具体数量门槛进行阐明。 国信办可参照 2020 年规范，其中列明了建议指定个人信息保护负责人的具体员工和数据主体数量。我们建议强制性门槛应高于"最佳做法"建议的数量门槛。
	(b) Differences between the positions required by the CSL and PIPL Article 21(1) of the CSL requires the appointment of a person in charge of cybersecurity. The respective roles and responsibilities of the positions required under the PIPL and CSL are not clear and it is unclear whether the appointment obligation under both the PIPL and CSL	We suggest harmonising the details on the positions required by the PIPL and CSL, either in the PIPL or its implementing regulations. In addition, to facilitate compliance by financial institutions, we recommend expressly clarifying:

Article 条款	Comments 意见	Recommendations 建议
	can be met through the appointment of a single individual.	• that the person in charge of personal information can share roles between group companies or other similar data protection roles under other laws or regulations; • if this role resides within the first-line function or second-line function, or if this determination is to be made by the organisation; • that the responsible person can have other roles; and • the clear obligations and potential liabilities of this person or providing reference to other guidance such as in the 2020 Specification.
	(b) 网络安全法与个人信息保护法要求的差异 网络安全法第 21(1)条要求指定网络安全负责人。个人信息保护法下的个人信息保护负责人和网络安全法下的网络安全负责人各自的职能和责任并不明确，因此不清楚是否可以只任命一人即可同时满足个人信息保护法和网络安全法的要求。	我们建议在个人信息保护法或其实施细则中对个人信息保护法和网络安全法下的岗位设置要求进行细节统一。 此外，为便利金融机构的合规，我们建议明确： • 个人信息保护负责人可同时承担集团各公司的个人信息保护负责人的职能，或其他法律法规要求的类似的数据保护职能； • 该职务属一线职能或二线职能，或可由组织自行决定； • 该负责人可同时具有其他职能；及 • 该人士的具体义务和潜在责任，或提述其他指南作为参照（例如 2020 年规范）。
52	PIPL requires an offshore processor that analyses or assesses the PRC individuals' behaviour to establish a dedicated agency or appoint a representative in China.	We recommend the appointment of a representative within China should only be required when a company processes personal information involving a threshold quantity of personal information or a substantial number of data subjects. In addition, Article 27(2) of GDPR

Article 条款	Comments 意见	Recommendations 建议
		provides exemptions to certain types of incidental or inadvertent processing. We recommend that the Commission may consider including such exemptions under the PIPL to avoid over-regulation.
52	个人信息保护法要求分析、评估中国境内自然人行为的境外信息处理者须在中国境内设立专门机构或者指定代表。	我们建议仅在公司处理的个人信息达到一定数量门槛或涉及大量数据主体时，才需要在中国境内指定代表。 此外，GDPR 第 27(2)条对某些类型的附带或无意信息处理规定了豁免。我们建议法工委可考虑在个人信息保护法中加入此类豁免，以避免过度监管。
53	Article 53 imposes an audit requirement on all personal information processors. It is unclear what data the professional institutions will be expected to have access to and what confidentiality obligations they would operate under to give business confidence in respect of trade secrets and other sensitive information.	We recommend that the audit requirements only be required where a financial institution processes a threshold quantity of personal information or the information relates to a substantial number of data subjects. We also recommend prescribing clear limitations (either in the PIPL or its implementing regulations) on what data the professional institutions will have access to and what confidentiality obligations they would operate under.
53	第五十三条对所有个人信息处理者施加了一项审计要求。 不太明确的是：进行审计的专业机构将有权访问哪些数据以及将承担怎样的保密义务，以使企业确保其商业秘密和其他敏感信息的安全。	我们建议仅在金融机构处理的个人信息达到一定数量门槛或涉及大量数据主体时，才需要进行审计。 我们还建议（在个人信息保护法或其实施细则中）对专业机构有权访问的数据以及其应承担的保密义务作出明确规定。
54	Article 54 suggests a wide range of activities where risk assessment is required. However, we submit that some of these activities are “business as usual” operational activities. For example:	Please see the Financial Services Sector Cybersecurity Profile developed by the Financial Services Sector Coordinating Council[8] as an example of a risk-based assessment tool which may be useful reference for the Commission. The Cybersecurity Profile can be further

[8] 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
	• sending employee data to a multinational organisation's head office for employment management and employee benefits purposes; and • outsourcing operational activities to vendors/service providers, e.g. engaging insurance companies for employee insurance purposes. The requirements on risk assessments are onerous, and should be limited to only situations of high risk, or which may potentially result in material risk of harm to individuals. Additionally, ALL organisations are subject to the requirements under Chapter 5 (Articles 50 to 55) on data protection, which should apply to ALL aspects of personal information processing. We submit that complying with Articles 50 to 55 should mitigate the risks of personal information processing in "business as usual" situations.	updated to include mapping of local efforts to support those operators within China We recommend taking a risk-based approach, which would help promote innovation in the technology sector, while still ensuring the appropriate level of protection. Article 54 should be revised to require risk assessments to be conducted, and records to be retained, only in situations which are likely to result in high risk or material risk of harm to individuals. As for ADM, we propose that the risk assessment be triggered only if the use of ADM "produces legal effects concerning him or her or similarly significantly affects him or her" and where solely ADM is used. This is in line with international norms, including the GDPR (Article 35.3(a)).
第五十四条	根据第五十四条，需要对大量的活动进行风险评估。但我们认为，其中某些活动属"惯常业务过程中"的经营活动。例如： • 因雇用事务管理和员工福利而将雇员资料发送给跨国机构的总部；和 • 将经营活动外包给厂商/服务提供者（例如，为员工保险而聘用保险公司）。 风险评估要求略显苛刻，应仅适用于高风险情形或可能导致重大的个人权益损害风险的情形。 此外，**所有**组织均须遵守第五章（第五十条至第五十五条）关于个人信息保护的要求。该等要求适用于个人信息处理的**所有**方面。我们认为，遵守第五十条至第五十五条规定，应已减少了"惯常业务过程中"个人信息处理方面的风险。	有关风险为导向的评估方法，请参阅美国金融服务行业协调委员会编撰的《金融服务行业网络安全概况》。这对法工委可能是有用的参考资料。可在该网络安全概况的基础上结合中国实践进行更新，以更好地为中国境内经营者提供支持。 我们建议采用风险为导向的评估方法，这有助于促进技术创新，又能确保保护水平处于适当程度。 第五十四条条文应作调整，只有在高风险情形或可能导致重大的个人权益损害风险的情形下，方要求进行风险评估并保留相关记录。 对于自动化决策系统，我们建议，只有在自动化决策"会产生涉及到个人的法律后果或对个人产生类似的显著影响"而且仅使用自动化决策系统的情形下，方会触发风险评估。这与国际规范（包

Article 条款	Comments 意见	Recommendations 建议
		括 GDPR（第 35.3(a)条））是一致的。
55	Article 55 requires notification to be made to the relevant authorities and impacted individuals for ALL data breaches. We submit that this threshold is too low, as it would include accidental disclosures of non-sensitive personal information where there is no impact or risk of harm to individuals. Such a reporting regime would result in over-reporting, create extensive administrative overheads for both authorities and organisations, and inevitably desensitise authorities and individuals to reports of incidents that indeed may have a major impact. Also, the concept of a "personal information leak" is not clearly defined under the PIPL, so it is difficult for financial institutions to know what amounts to the appropriate notification trigger. In addition, the timeframe for making the notification is not clear under the PIPL. Currently, the PIPL states that notification must be made immediately following the identification of a data breach but, in practice, this would be impractical for financial institutions to comply with. Financial institutions need time to ascertain how the breach occurred, access the preliminary impact and materiality, potentially conduct a forensic investigation through hiring outside experts, understand what action must be taken internally to restore the reasonable integrity of the affected system, and gather accurate information to be reported to the relevant parties. This can take many days, if not weeks, to complete.	We recommend clarifying the scope of a "personal information leak" that must be reported by adopting a risk-based approach and requiring mandatory notification only where there is the potential for significant risk of harm to the impacted individuals. Such an approach would also allow organisations and authorities to focus resources appropriately on matters of material risk. In addition, we recommend that financial institutions should be required to notify their designated supervisory authority in line with existing financial regulation/ guidance (e.g. the PBOC). We also recommend that the Commission add a reasonable timeframe to assess the severity of the breach in advance of providing notification to the authorities and individuals. We understand that many financial institutions and other organisations have reported that the 72-hour timeframe provided under the GDPR is unrealistic and impracticable for most breaches.

Article 条款	Comments 意见	Recommendations 建议
第五十五条	第五十五条规定，应就**所有**的个人信息违规行为通知相关部门和受影响的个人。我们认为，这一门槛太低，因其将没有影响或危害到个人的非敏感个人信息的意外泄露也包括在内。 这样的通知制度将导致过度通知，为相关部门和通知主体增加大量行政开支，不可避免地使相关机构和个人对确实会产生重大影响的事件通知失去敏感性。 此外，没有对个人信息保护法下“个人信息泄露”作出清晰界定，致使金融机构难以知晓何种金额水平属触发申报机制的适当水平。 另外，作出通知的时间表在个人信息保护法中也不明确。目前个人信息保护法的规定是在发现个人信息泄露后立即作出通知，但在实践中金融机构很难遵守这一要求。因为它们需要时间确定泄露是如何发生的，对影响和严重性进行初步评估，可能还需聘请外部专家进行取证调查，了解内部须采取的措施以恢复受影响系统的合理完整性，并收集准确的信息以报告给有关各方。完成此过程可能需要几天甚至几周的时间。	我们建议，应采用风险为导向的评估方法对必须通知的“个人信息泄露”所涵盖的范围作出清晰界定；只有可能存在重大的个人权益损害风险的情形下，才须强制通知。这样的方法也有助于申报主体和相关部门适当地将资源重点投放到重大风险事项上。 此外，我们建议，金融机构应遵循现有的金融法规/指引向指定的监管机构（例如央行）进行通知。 我们还建议法工委给予一段合理的时间以便金融机构在通知有关部门和个人之前能对泄露的严重性进行评估。我们理解，许多金融机构和其他组织都提出，对于大多数泄露事件，GDPR 规定的 72 小时时间表是不现实及不切实际的。
Chapter VI Authorities Fulfilling Personal Information Protection Duties and Responsibilities **第六章 履行个人信息保护职责的部门**		
56	This article provides that the following constitute “authorities fulfilling personal information protection duties and responsibilities”: (a) the CAC is responsible for comprehensive planning and cooperation; (b) the relevant authorities under the State Council are responsible for personal information protection, supervision, and management within their respective scope; and (c) the relevant authorities of the people’s	We make the following recommendations here: **(a) One centralised regulator** We recommend that observance of data protection obligations of financial institutions should be supervised by a single regulator (or at least one primary regulator) to ensure consistent interpretation and enforcement of the PIPL requirements. We recommend that the lead regulator for financial institutions should be the PBOC, an authority that would know the

Article 条款	Comments 意见	Recommendations 建议
	government at or above the county level shall fulfil the personal information protection, supervision and management duties and responsibilities determined pursuant to relevant state regulations. This raises concerns that there could be inconsistent interpretation and enforcement of the PIPL by the different authorities. The potential differences in legal and regulatory requirements regarding personal information security and management across different sectors and different regions in the PRC is an area of focus and concern which may deter investment into the PRC.	intricacies of the existing and new rules. **(b) Involvement of local governments** We suggest clarifying the local governments' involvement (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 the same personal information which may be used in multiple locations. **(c) Details on how different authorities will cooperate with each other** We suggest clarifying the definition of coordination to avoid duplicative actions and penalties where one financial institution is subject to the supervision of multiple authorities.
第五十六条	本条规定“履行个人信息保护职责的部门”构成如下： (a) 国信办负责统筹协调工作； (b) 国务院有关部门在各自职责范围内负责个人信息保护和监督管理；及 (c) 县级以上地方人民政府有关部门应根据国家有关规定履行个人信息保护和监督管理职责。 我们担心此规定会导致不同部门对个人信息保护法的解释和执法不一致。 中国不同行业和地区在个人信息安全和管理相关法律和监管规定方面的潜在分歧势必会引发关注和关切，有碍投资进入中国。	我们的建议如下： **(a) 统一的中央监管机构** 我们建议由统一的监管机构（或至少指定一个主要监管机构）监督金融机构遵守个人信息保护义务，确保对个人信息保护法相关规定的解释和执法保持一致。 我们建议由熟悉现有法规和新法规之间复杂联系的央行担任金融机构的牵头监管者。 **(b) 地区政府的参与** 我们建议对地方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），并说明地方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个人信息在不同地区遵守不同规则，在实际执行中将面临困难。 **(c) 不同机构之间具体如何相关合作** 我们建议对机构间协调合作作出清晰说明，以避免对一家受多个部门监管的金融机构采取重复行动和作出重复处罚。
57(3)	We submit that this article does not provide sufficient details relating to who may exercise such powers in respect of a particular industry such as the finance industry.	We suggest clarifying the relevant authorities. We reiterate our comments and recommendations that any investigatory power should not cover non-PRC processing activities other than to the extent necessary to meet a narrow scope of extraterritorial supervision in line with practice in other international markets.
第五十七条第三款	我们认为，对于诸如金融业等特定行业，本款对于职责主体的规定不够充分具体。	我们建议对相关部门作出清晰界定。 重申我们的意见和建议：任何调查权均不应涵盖非中国境内的信息处理活动，但属根据其他国际市场的惯例，为满足有限域外监管而必需的除外。
58	We note that the CAC and the relevant authorities under the State Council are responsible for formulating personal information-related rules and standards.	We reiterate out comments in relation to Article 11 that these standards should adopt existing international standards and best practices.
第五十八条	我们注意到，国信办和国务院有关部门均负责制定个人信息相关规则和标准。	我们重申有关第 11 条的意见，即该等标准应采用现有的国际标准和最佳做法。
59	We submit that the second paragraph of this article does not provide sufficient details relating to how the authorities fulfilling personal information protection duties and responsibilities may exercise their power of investigation and enforcement.	We recommend providing specific details regarding how information may be collected by the relevant authorities and how they will make such requests for information, including details on: • how they may exercise their powers to request information stored outside the PRC for the purpose of investigating any harmful non-PRC

Article 条款	Comments 意见	Recommendations 建议
		processing activities; and • the approval procedures that they need to go through to the request information for the purpose of investigations.
第五十九条	我们认为，在履行个人信息保护职责的部门如何行使其调查执法权力方面，本条第二款的规定不够充分具体。	我们建议，就相关部门会如何收集信息以及会如何要求提供信息作出具体规定，具体包括以下两方面： • 对于任何非中国境内的违法行为，相关部门将如何行使其调查权并要求提供储存于中国境外的信息；及 • 相关部门为了上述调查而要求提供信息时所需履行的审批程序。
Chapter VII Legal Liability **第七章 法律责任**		
Chapter VI in general	NA	We suggest clarifying which competent authority (or authorities) will enforce the PIPL with respect to financial institutions.
第七章整体	不适用	我们建议，对于将由哪一主管机构对金融机构开展个人信息保护法下的执法行动，应作出清晰明确的规定。
61	Whilst enterprises will welcome a mechanism under which enquiries and complaints can be made to the relevant authorities, more detail of the processes is required to ensure transparency and accountability on the part of the authorities involved.	It would serve the interests of enterprises to clarify in the PIPL the process underlying this communication channel or set this detail out in implementing regulations to be published at the time of promulgation of the PIPL, so that financial institutions can better understand their rights in this regard. Moreover, defining inquiries and complaints to be addressed would support an organisation's timely response.
第六十一条	虽然企业非常欢迎设置这一向相关部门咨询和投诉的机制，但需要就这一机制作出更为具体的规定，以确保相关部门工作透明度和负责度。	在个人信息保护法中清晰规定这一沟通机制的基本流程，或在个人信息保护法颁布时所公布的相关实施细则中作出具体规定，将对于企业有所帮助。这样，金融机构可更好地理解其在这方面的权利。此外，对须予以处理的咨询和投诉

Article 条款	Comments 意见	Recommendations 建议
		作出详细界定，将有助于相关机构及时作出回复。
62	While we appreciate the government's desire to raise the importance of data protection compliance through meaningful sanctions for failure to comply, 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) Lack of clarification on the percentage fine** Serious violations of the PIPL may result in fines of up to RMB50 million or 5% of the annual revenue of the previous year. However, it is not clear how the percentage fine would be calculated.	We recommend clarifying what amounts to a serious violation and that the calculation method for the percentage fine is by reference to the enterprise's domestic revenue, so that enterprises can properly understand their risk exposure for non-compliance.
第六十二条	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个人信息保护合规的重要性，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的具体数额应当完全透明且不含糊。 **(a) 按百分比计算罚款的规定不够清晰明确** 违反个人信息保护法且情节严重的，处人民币五千万元或者上一年度营业额百分之五以下罚款。但是，按百分比计算罚款的计算的计算方式没有予以明确。	我们建议对何为情节严重作出清晰规定，并明确按企业中国境内营业额的百分比计算罚款，以便企业可以正确理解其不合规的风险。
	(b) Lack of clarification on the "officer directly in charge" and "other directly responsible personnel" The "officer directly 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 the processing of personal information. Given the magnitude of	We suggest clarifying the definitions of "officer directly in charge" and "other directly responsible personnel". We also recommend that the threshold for the individual liability should 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

Article 条款	Comments 意见	Recommendations 建议
	personal liability involved, it is crucial for senior management of financial services firms to understand the scope of these terms.	roles.
	(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个人信息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巨大，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。	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，触发个人法律责任的门槛应予以明确，并应设置在充分高的水平（例如，欺诈和故意违法而非单纯的疏忽），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。
70	We note that no timetable is stated for the effectiveness of the PIPL.	We suggest that the period should be at least 24 months from finalising the form of the PIPL. If, for any reason, relevant sectoral rules cannot take effect at the same time as the PIPL, 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.
第七十条	我们注意到，个人信息保护法的生效日期尚未确定。	我们建议，生效日期应在个人信息保护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个人信息保护法同时生效，我们建议，相关行业规则最终确定后有一个 24 个月的过渡期，以确保金融机构完全了解相关影响并制定和实施必要的合规措施。