28 May 2021

2021 年 5 月 28 日

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

No.1 Qianmen West Street, Xicheng District

Beijing, China

100805

全国人大常委会法制工作委员会

西城区前门西大街 1 号

北京，中国

邮编：100805

To the Commission

致：法工委

Consultation Draft of the Second Review of the Personal Information Protection Law

《个人信息保护法》（草案二次审议稿）征求意见

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

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

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

与《个人信息保护法》（草案一次审议稿）征求意见（"**个人信息保护法（草案一次审议稿**"）相同，协会已征求协会会员意见并得到积极回应。本函件载列我们关于个人信息保护法（草案二次审议稿）的意见、金融机构可能面临的实际困难、我们的建议以及我们对个人信息保护法（草案二次审议稿）若干条文明晰化的请求。

---

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

ASIFMA 是一个独立的区域性行业协会，会员基础广泛，由银行、资产管理公司、律师事务所和市场基建服务供应商等 140 多家来自买方和卖方市场的领先金融机构和专业机构组成。我们在金融行业拥有共同的利益，即促进在亚洲建立发展一个流动性强并具有深度和广度的资本市场。ASIFMA 认为拥有一个稳定、创新、竞争和高效的亚洲资本市场对于支持亚洲地区的经济增长是十分关键的。我们通过汇聚集体力量和统一行业发声，围绕关键问题推动形成共识、提出解决方案建议并促成变革。我们采取的努力包括与监管机构和交易所进行磋商、制定统一的行业标准、通过政策文件推动改善市场，并降低在地区内开展业务的成本。ASIFMA 通过全球金融市场协会（GFMA）与美国的证券业与金融市场协会（SIFMA）及欧洲的金融市场协会（AFME）形成联盟，共同提供全球最佳行业实践及标准，为区域发展作贡献。

[2] Available at: http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80818178f9100801791b35d78b4eb4.
可于以下网址查阅:
http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80818178f9100801791b35d78b4eb4。

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 Second Review PIPL – as was the case for the First Review PIPL – casts a broad net and, 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 particular the Cybersecurity Law ("**CSL**") and the Data Security Law (draft) ("**DSL**") – is also unclear.

同时，与个人信息保护法（草案一次审议稿）相同，个人信息保护法（草案二次审议稿）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**。

Next steps

下一步行动

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

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

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

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

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

本函件在昭胜年利达（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！

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

Appendix – Detailed comments

附件 – 具体意见

Introduction

绪言

This Appendix is structured as follows:

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 Second Review PIPL; any reference to the "**Second Review PIPL**" is a reference to the draft of the Personal Information Protection Law ("**PIPL**") published on the National People's Congress website as at the date of this submission; and any reference to an Article is to an Article of the Second Review PIPL.

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（草案二次审议稿）解释。"**个人信息保护法（草案二次审议稿）**"指截至本函件日期在中国人大网所登载的《个人信息保护法》（"**个人信息保护法**"）草案；凡提及某一条款之处均是指个人信息保护法（草案二次审议稿）中的条款。

Part A Overarching comments

甲部 整体意见

1. Principle-based obligations

原则性义务

We understand that the 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 2021 China Business Climate Survey Report released by AmCham China,[3] which noted that inconsistent regulatory interpretation and unclear laws and enforcement is a top challenge for the services sector.

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

We recommend the Commission consider:

我们建议法工委考虑下列各项：

(a) having a lead, or coordinating, regulator (e.g. the People's Bank of China ("**PBOC**")) in implementing the 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（如中国人民银行（"**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；

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

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

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

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

按行业应用的规则、法规或指引（"**行业规则**"）的适用性应优于：

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

个人信息保护法框架内的规则。具体而言，并非在某一条文或规定中提及行政规章将在哪些领域优先适用，而应明确说明按行业实施的规定具有补充性，其适用性优于个人信息保护法等原则性法律；及

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

任何金融行业新制定的行业规则应替代或是明确补充现行规则以避免范围重叠；及

(e) that sectoral rules take effect at the same time as the 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。

In addition to supplementing the framework of the PIPL with sectoral rules, if one of the purposes of the Commission is to truly create a framework that makes the PRC competitive with other financial markets, it is crucial to allow financial institutions and other businesses operating in the PRC to comply with, and streamline processes based on, international standards. To this end, it is crucial that the PIPL recognises international standards in addition to their domestic equivalents, especially to facilitate cross-border data flows and support multinational financial institutions. National standards for personal information protection formulated by the Cyberspace Administration of China ("**CAC**") and other relevant authorities need to be made compatible with existing international standards. Guidance in this regard should be developed with the PBOC and other financial regulators for financial institutions, including exceptions in the context of processing personal information and data transfers for effective risk management and meeting existing regulatory obligations.

除通过行业规则补充个人信息保护法的框架外，如果法工委的目的之一是真正创建一个框架，使中国与其他金融市场一样富有竞争力，则至关重要的是允许中国境内运营的金融机构和其他企业遵守国际准则并基于国际准则优化流程。为此，重要的是个人信息保护法认可在国内同等规范之外存在的国际准则，特别是为跨境数据流动提供便利并支持跨国金融机构。国家互联网信息办公室（"**国信办**"）和其他有关机构制定的国内个人信息保护准则需要与现行国际准则兼容。就此方面，应与央行等金融监管机关为金融机构制定指导意见，包括为进行有效的风险管理和符合现有监管义务而处理个人信息和数据转移情况下的例外情形。

2. Overlap with existing laws and regulations

与现有法律法规重叠

The wide scope of application of the PIPL causes overlap with existing laws, regulations and guidelines. For example, the CSL covers "*network data*" which refers to *"all kinds of electronic data collected, stored, transmitted, processed and*

produced through the networks". Where there is any inconsistency in the overlapping parts among the 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. Similarly, the Civil Code of the PRC, which took effect on 1 January 2021, contains provisions relating to personal data protection and privacy.

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。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网络安全法及其附属法律及指引之间有任何不一致或重叠部分，则如何应用"*特别法优于一般法*"或"*新法优于旧法*"的原则将存有疑问。同样，自 2021 年 1 月 1 日生效的中国民法通则载有关于个人数据保护和隐私的条款。

In addition, laws that are in the pipeline have an apparent overlap with the PIPL, in particular the DSL for which the second public consultation process is being completed in parallel with that of the PIPL.

此外，在审议过程中的其他法律与个人信息保护法有明显的重叠，尤其是与个人信息保护法同时完成第二次向社会公众征求意见程序的数据安全法。

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

我们促请法工委优先检视可能会与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。[4] 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。我们尤其建议具体说明下列各项（或提供辅助指引）：

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

如果有与其他法律、法规或指引不一致的情况，将会如何处理；及

(b) how the 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。

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

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

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

数据本地化和个人信息跨境传输

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 ("**AML**") and counter-financing of terrorism ("**CFT**") laws and regulations through leveraging global service centres. Localisation does not improve data protection. Instead, localisation requirements introduce technical complexity and additional administrative layering into corporate operations, both of which ultimately compromise the effectiveness of cybersecurity and risk management controls.

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（"**反洗钱**"）和反恐怖主义融资（"**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:

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：

(a) if the Commission strongly believes that such security assessments are required under the new regime, at a minimum, there is a need for clarity on exactly what a security assessment and professional accreditation process entails;

如果法工委坚信在新制度下需要该等安全评估，则至少必须明确安全评估和专业认证程序究竟需要什么；

(b) introducing an express exception 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;

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；

(c) relaxation of any requirement to use the exact standard contract clauses proposed by regulators, provided that the contracts implemented by financial institutions provide equivalent protection to the template clauses. Alternatively, regulators should provide a general description of the clauses that contracts must cover and use of the standard contract clauses may be used by organisations as a guidance document only;

如金融机构实施的合同应为模板条款提供了同等保护，放宽须使用监管机构建议的明确标准合同条款的要求。或者，监管机构应就各合同必须涵盖的条款提供一个一般说明，而组织可仅将标准合同条款作为一个指导文件使用；

(d) removing the requirement that "processors processing personal information above a certain threshold" must store data within the PRC; and

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中国境内的要求；及

(e) significantly narrowing the scope of personal information that may require prior approval from the competent PRC authorities before that information can be transferred offshore to a foreign law enforcement agency or judicial body.

将可以出境给外国执法机关或司法机构之前须获得中国主管机构事先批准的个人信息范围大幅缩小。

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

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

4. Processing grounds

处理依据

We strongly welcome the introduction under the PIPL of additional statutory processing grounds, other than obtaining the consent of a data subject, to be able to collect and process his or her personal information. However, 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.

我们非常欢迎个人信息保护法下除了取得数据主体同意以收集和处理其个人信息外还引入额外的法定处理依据。但是，我们也关注到个人信息保护法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。

First, 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, this additional burden is highly impractical for businesses in the finance sector (and other consumer sectors) if it cuts across the processing grounds set out in Article 13. 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，如果超出第十三条所述的处理依据，这一额外负担对金融业（和其他消费行业）的企业来说是非常不切实际的，而且有理由相信，频繁地寻求客户同意会不必要地损害客户体验，而非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。

Further to the above, separate consent is required from individuals where a personal information processor engages another party to process the personal information. It would not be practicable to notify individuals of the identity of each third-party recipient, the contact information of the third party, and the processing method. 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 the European Union's General Data Protection Regulation ("**GDPR**").

除上述者外，个人信息处理者委托另一方处理个人信息的，须向个人取得单独同意。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。我们建议，向个人告知接收人的类别而非接收人的确实身份。这符合国际规范，包括欧盟的《通用数据保护条例》（"**GDPR**"）。

5. Extraterritoriality

域外法权

The potential reach of the PIPL may impose a significant burden on international financial institutions. In particular, the PIPL covers:

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。尤其是个人信息保护法涵盖：

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

在中国境内开展的数据活动（"**中国境内数据活动**"）；

(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**").

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 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 wider 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，导致企业的各项法律义务相互冲突，因此金融机构及整个业界极为关注。

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

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。

More specifically, the application of the PIPL to activities of organisations and individuals outside the PRC is very difficult to apply without clear and objective parameters that can be reasonably assessed by those persons. As drafted, the extraterritorial reach is disproportionate to the potential risk, given there may be very limited PRC nexus (if at all) with data potentially collected and stored wholly outside 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. Since the First Review PIPL, our membership has emphasised that the implementing rules of the GDPR should be noted as further discussing how extraterritoriality is aimed only at an intentional, targeted offering of goods or services to individuals in the EU, as opposed to where the provision of goods or services is incidental or inadvertent. As for the First Review PIPL, we urge that the PIPL must prescribe similar indications to those in the GDPR as to the extent of its extraterritorial application on the offering of goods or services.

具体而言，如果中国境外的组织和个人无法以明确客观合理地作出评估，那么中国境外的组织和个人将难以应用个人信息保护法于其开展的活动。根据草案，域外应用范围与潜在风险不成比例，并可能与中国的关联非常有限，且可能包含完全在中国境外收集和存储的数据。倘中国相关机构希望在向中国提供商品或服务方面遵循

国际模式，则企业了解这些规则的应用范围至关重要，并确保偶然和无意的活动不在其范围内。自从个人信息保护法（草案一次审议稿）以来，我们的成员一直强调，应注意 GDPR 的实施规则的域外法权仅针对有意、有针对性地向欧盟个人提供商品或服务，而不是附带或无意地提供商品或服务。关于个人信息保护法（草案一次审议稿），我们促请个人信息保护法必须就其对商品或服务提供方面的域外适用范围参照 GDPR 中类似的规定。

Furthermore, as noted above, the PIPL's jurisdictional reach also exceeds that of the CSL. We submit that the extraterritorial application of the existing CSL is sufficient to 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 among foreign financial institutions. We believe restricting the PIPL's extraterritorial application to a smaller scope or one that is commensurate with the CSL, may help alleviate these concerns. In particular, we strongly suggest that areas of law covering a common overall subject matter should be consistent in their application.

此外，如上文所述，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同的范围有助缓解此问题。尤其是，我们强烈建议涉及同一类目标整体的法律领域应采用统一的应用标准。

Finally, where certain provisions are *not* intended to apply to 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，对中国境外开展的数据处理活动不适用的部分条文，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。

6. Data Breach Notification

数据违法通知

Our members appreciate there is a general trend towards mandatory breach reporting in Asian and other data protection regimes. This trend serves the purpose of driving transparency among businesses and consumers.

我们的成员理解到亚洲和其他数据保护制度普遍存在对数据违法进行强制性通知的趋势。这一趋势的目的是提高企业和消费者之间的透明度。

However, we believe that notifications should only be triggered by breaches assessed by financial institutions and other organisations to be sufficiently significant on a risk-based assessment to warrant reporting. For example, a risk-based approach might be based on the nature of data impacted, the number of affected persons, whether malice was involved, etc.

但是，我们认为，仅应在金融机构和其他组织在风险导向评估上评估违法行为具有足够的重要性需要作出通知时，才应触发通知。例如，风险导向方法可以基于受影响数据的性质、受影响的人数、是否涉及恶意等。

As presently proposed, the lack of a threshold below which reporting is not required under the PIPL would result in accidental disclosures of non-sensitive personal information (even within the same corporate group) having to be reported despite these not impacting or risking harm to individuals. Such a reporting regime would result in over-reporting, create extensive administrative overheads for both authorities and financial institutions and other organisations, and inevitably desensitise authorities and individuals to reports of incidents that indeed may have a major impact.

如目前所建议，在个人信息保护法项下，如果没有一个不需要通知的下限，将导致必须披露非敏感个人信息（即使在同一公司集团内）的意外泄露，尽管披露这些信息不会对个人造成影响或伤害。此种通知制度将导致过度通知，为主管机构及金融机构和其他组织均造成大量的行政管理费用，且不可避免地使主管机构和个人对确实会产生重大影响的事件作出通知失去敏感性。

We recommend clarifying the scope of a “personal information leak” that must be reported only relates to cybersecurity breaches where there is the potential for significant risk of harm to the impacted individuals. A risk-based approach would then allow organisations and authorities to focus resources appropriately on matters of material risk.

我们建议将必须通知的“个人信息泄露”所涵盖的范围清晰界定为仅涉及可能对受影响个人造成重大损害风险的网络安全方面的违法，风险导向评估方法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。

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**		
1	In the opening principles of the Second Review PIPL, the statement that the PIPL is formulated to safeguard the orderly and free flow of personal information is removed from the provision that was set out in the First Review PIPL. While we appreciate that there will need to be certain restrictions in place to protect certain interests including national security and individuals' privacy, we submit that the free flow of personal information should remain a core tenet of the PIPL.	We recommend that a statement emphasising the PRC's desire to foster a digital ecosystem founded on free flow of information be reinstated, with caveats as necessary to show commitment to this principle – in particular as this principle was agreed as recently as November 2020 with the PRC's agreement of the Regional Comprehensive Economic Partnership, including commitments on cross-border transfers of data in Chapter 12.
第一条	在个人信息保护法（草案二次审议稿）的开篇总则中，关于制定个人信息保护法是为了"保障个人信息依法有序自由流动"的声明被删除，而这一声明曾在个人信息保护法（草案一次审议稿）的规定当中。 虽然我们理解需要有一定的限制来保护某些利益，包括国家安全和个人隐私，但我们认为，个人信息的自由流动应仍然是个人信息保护法的核心原则。	我们建议恢复强调中国希望建立一个以信息自由流动为基础的数字生态系统的声明，作为表明对这一原则承诺的必要说明。特别是，近期在 2020 年 11 月，中国签署了《区域全面经济伙伴关系协定》（包括其第十二章就跨境数据传输作出承诺）并就这一原则达成一致。
3	**(a) Location of individuals protected** The Second Review PIPL continues to apply 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	**(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.

	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 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) Provision of products or services in the PRC** We submit that the current concept of "provide any product or service … in the People's Republic of China" under item 2 of Article 3 is extremely vague, such as may include a wide range of activities that are not intended to be in scope of the PIPL. **(c) Broad scope of "analyse or assess" as processing activities** We submit, as for the First Review PIPL, that the current concept of "analyse or assess the behaviour of natural persons in the People's Republic of China" 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 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	**(b) Narrowing down the scope of products or services** We recommend that further explanation is given as to the meaning of providing products or services in the PRC. For example, under Article 3.2 of the Guidelines for Data Cross-border Transfer Security Assessment (Draft), a list of factors was suggested such as the use of Chinese, or settlement in renminbi. Financial institutions need clarification to understand how the operation of affiliated entities or other global support units overseas is treated under the PIPL. **(c) Narrowing down the scope of "analyse or assess"** We recommend that, to avoid unintentionally catching the legitimate operational needs of multinational financial institutions, the PIPL or implementing regulations to be published at the time of promulgation of the PIPL clarify the types and/or purposes of behaviour, analyses and assessments that should be outside the scope of item 2 of Article 3 (for example, random searches on PRC individuals conducted outside the PRC, and other activities covered in a permitted activities list and/or covered by Article 13). **(d) Deletion of catch-all provision** As was an important issue for financial institutions in the First Review PIPL, 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

	Information security technology: personal information security specification (GB/T 35273-2020) (the "**2020 Specification**"). **(d) Catch-all provision** We also submit. as for the First Review PIPL, 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 the processing activities of financial institutions outside 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. **(e) Wide application of PIPL** Though Article 71 of the Second Review PIPL (previously Article 68 of the First Review PIPL) 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).	application should be clearly designated for enterprises and individuals. In particular, though the concepts set out in this article are like those under the GDPR, the GDPR and its implementing rules and supporting case law also seek to provide further detail on, for example, when an overseas business operator could be seen as offering goods and services in the EU. Since the First Review PIPL, our membership has further emphasised that the implementing rules of the GDPR should be noted as further discussing how extraterritoriality is aimed only at an intentional, targeted offering of goods or services to individuals in the EU, as opposed to where the provision of goods or services is incidental or inadvertent. As for the First Review PIPL, we urge that the PIPL must prescribe similar indications to those in the GDPR as to the extent of its extraterritorial application on the offering of goods or services. **(e) 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.
第三条	**(a) 受保护个人的地点** 个人信息保护法（草案二次审议稿）继续适用于"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	**(a) 明确受保护个人的范围** 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) 缩小产品或服务的范围** 我们建议就"…向境内自然人提供产品或者服务…"的含义作出进一步解释。例如，在《数据出境安全评估指南》（草案）第 3.2 条项下提出了一系列参考因素，如使用中文及以人民币结算等。金融机构需要澄清以便了解根

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) 在中国境内提供产品或服务

我们认为，目前第三条第二款中"…向境内提供产品或者服务…"的概念极为模糊，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。

(c) "分析或评估"作为处理活动的范围的宽泛性

我们认为，与个人信息保护法（草案一次审议稿）一样，目前第三条第二款项下关于"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《信息安全技术：个人信息安全规范》（GB/T 35273-2020）（"**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。

(d) 总括性条款

我们还认为，与个人信息保护法（草案一次审议稿）一样，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。

(e) 个人信息保护法的宽泛适用

尽管个人信息保护法（草案二次审议稿）第七十一条（原个人信息保护法（草案一次审议稿）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。

据个人信息保护法，如何对待关联实体或其他海外全球支持单位的运营。

(c) 缩小"分析或评估"的范围

我们建议，为避免无意间妨碍跨国金融机构的合法运营需求，个人信息保护法或在个人信息保护法颁布时公布的个人信息保护法实施条例明确在第三条第二款范围以外的行为，"分析、评估"的类型和/或目的（例如，在中国境外对中国个人进行的随机搜索，以及在允许的活动清单和/或第十三条中包含的其他活动）。

(d) 删除总括性条款

作为金融机构在个人信息保护法（草案一次审议稿）中关注的一个重要问题，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，虽然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同样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。自个人信息保护法（草案一次审议稿）以来，我们的成员进一步强调，应注意到 GDPR 的实施细则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。与对于个人信息保护法（草案一次审议稿）一样，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与 GDPR 类似的规定。

(e) 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。

	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）。	
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. In these definitions, the use of terms like "etc.", 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。在这些定义中，如果没有明确定义，则应避免使用"等"之类的表述，因为在实践中它们很难适用，且存在适用不一致的很大风险。	**(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。
8	The Second Review PIPL introduces an obligation on data processors to ensure the "quality" (质量) of personal information being processed. This term is vague and includes a sense of positive value, whereas businesses can (and often should) be agnostic to the subjective value or meaning	We recommend that the concepts of "accuracy" and being "up-to-date", as seen in the First Review PIPL, are returned to, unless the Commission can provide elaboration as to the intention and meaning behind the revisions to this article.

	underlying particular items of personal information.	
第八条	个人信息保护法（草案二次审议稿）为数据处理者规定了一项义务，即确保被处理的个人信息的“质量”。该术语含义模糊，包括一种积极的价值感，而企业可能（并且通常应该）不了解个人信息特定项目的主观价值或含义。	我们建议，除非法工委能够详细说明对本条所作修订的意图和含义，否则应恢复个人信息保护法（草案一次审议稿）中所述的“准确”和“更新”的概念。
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 by, for example, explicit reference to these measures being those mandatory requirements “stipulated under the PRC Cybersecurity Law and other applicable regulations”.
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”，例如，明确提及是“中国网络安全法及其他适用法规规定的”强制性要求。
10	The DSL is formulated, among others, to safeguard state sovereignty and national security (according to Article 1 of the DSL). Therefore, the prohibition on organisations and individuals processing personal information in a manner which is prejudicial to “national security or public interests” overlaps with obligations provided under the DSL (as continues to be the case for the second review draft of the DSL (“**Second Review 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 standards 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 duplicative and should be deleted to avoid creating confusion through overlapping obligations. This is a more general issue that should be addressed through the DSL (as is also asserted in our comments on the DSL being submitted to the Commission in parallel to this letter). **(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（数据安全法（草案二次审议稿）（“**数据安全法（草案二次审议稿）**”）的情况仍然如此）。 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。	**(a) 删除重复性概念** 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是重复规定，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（正如我们在随本函提交法工委的对数据安全法的建议中所述）。 **(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. Implementation of global standards and other systems is crucial to developing the PRC financial market and attracting foreign investors. This approach 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	As for the First Review PIPL, 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

	regulatory obligations, which will pose a significant challenge to multinational financial institutions.	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 extraterritoriality of the PIPL, we recommend that the government establishes the system for personal information protection 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。 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。这一做法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。	与对于个人信息保护法（草案一次审议稿）一样，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）自愿参与的个人信息保护制度，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. As many of our members operate on a multi-	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

	jurisdictional basis, we fully support this approach to exchange and cooperation.	personal information under Chapter 3 and elsewhere in the PIPL.[5]
第十二条	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。由于我们许多成员在多个司法管辖区开展业务，我们完全支持这种交流与合作。	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。[5]
Chapter II Rules on Processing of Personal Information **第二章 个人信息处理规则**		
13	**(a) Processing grounds lack practicality** We note that more grounds for collecting and processing personal information have been introduced under the PIPL and a further ground has been added in the Second Review PIPL compared to the First Review PIPL. However, there remains 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 six out of the eleven exceptions to consent under the 2020 Specification have been included under the Second Review PIPL (albeit one more than in the First Review PIPL). In addition, more practical processing grounds are seen in the data protection regimes of other financial centres in Asia [6] .	**(a) Business-friendly processing grounds needed** As for the First Review PIPL, 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

[5] 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）论坛建立的跨境隐私规则（CBPR）系统：http://cbprs.org/。

[6] 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）允许关于某一个人的个人资料在多种情形下（例如该等个人资料已经为公开可得），可以未经同意而被使用。类似地，在香港《个人资料（私隐）条例》下，只

	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.)). One obvious example being the personal information of a client organisation's representatives or other personnel that might be transferred as part of the information relating to the organisation (by reason of their role or involvement in the organisation), but the individual would have no expectation of needing to give consent to that transfer in such a scenario. Separately, in the context of the collection and processing of personal information in an electronic form through a network, it is 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. Although Article 13 of the Second Review PIPL is expanded to, we understand, explain that the processing grounds other than consent set out in Articles 13(2) to (7) override the need to obtain consent	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]. Also as for the First Review 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 of, 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

要数据主体获得告知，则为企业的职能及活动而收集和使用资料在一般情况下即被允许（《个人资料（私隐）条例》附表 1，资料保护原则，第 1 原则）。

[7] One illustrative example is provided by article 13 of the State Council's Administrative Regulations for Credit Services which states that "Information relating to the performance of duties by directors, supervisors and senior management personnel of an enterprise is not be personal information" and therefore no consent is required to process such personal information.

国务院《征信业管理条例》第十三条举了一个例子，该条规定："企业的董事、监事、高级管理人员与其履行职务相关的信息，不作为个人信息"，因此处理该等个人信息不需要征得同意。

	under other articles of the PIPL, it remains somewhat contradictory with the implication of Article 14, which maintains that other laws and administrative regulations shall prevail where they require a "separate consent" or "written consent". **(b) Processing ground for publicly available information** We note that a new processing ground is added in the Second Review Draft, as an exception to obtaining consent where personal information "is publicly available and the processing is within a reasonable scope and in accordance with the [PIPL]". This condition is therefore qualified compared to that under Article 5.6(f) of the 2020 Specification which does not have a concept of "reasonableness". While reading Article 13(5) alongside Article 28 suggests that there must be a relationship between the processing and the original purposes for which the personal information was originally published, this is not clear from the drafting of Article 13(5).	crucial in enabling international financial institutions to meet their compliance obligations (and such compliance is frequently monitored by the financial regulators in China). Also, please see our comments on Article 14 on indirect acquisitions of personal information. **(b) Remove "reasonableness" qualifier** We suggest that, in line with the 2020 Specification which contains processing grounds welcomed by financial institutions from the perspective of conducting key functions efficiently using digital tools for the purpose of AML compliance and increasing customer satisfaction, the concept of "reasonableness" is removed from Article 13(5). However, if the Commission maintains that the concept is necessary to protect individuals' interests, it will be important for financial institutions and other businesses to better understand the expectation on them to comply with the qualification of what is or is not "reasonable" processing.
第十三条	**(a)处理依据缺乏可行性** 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，与个人信息保护法（草案一次审议稿）相比，个人信息保护法（草案二次审议稿）中新增一项依据。但是仍然没有任何等同于 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 6 项已包括在个人信息保护法（草案二次审议稿）之中（尽管比个人信息保护法（草案一次审议稿）多一项）。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	**(a) 需要对业务友好的处理依据**

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。一个明显的例子是，一个客户组织的代表或其他人员的个人信息（由于其在该组织中的作用或其参与）可能作为与组织有关的信息的一部分而被转移，但在这种情况下，个人不会期望需要就这种转移作出同意。

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。我们理解，虽然个人信息保护法（草案二次审议稿）第十三条扩大为将第十三条中除第（二）项至第（七）项规定的除同意以外的其他处理依据优先于个人信息保护法其他条款所规定的需要取得的同意，但与第十四条的含义仍有一定的冲突。第十四条规定，其他法律和行政法规要求取得“单独同意”或者“书面同意”的，从其规定。

(b) 公开信息的处理依据

我们注意到，在个人信息保护法（草案二次审议稿）中增加了一项新的处理理由，作为获得同意的例外情况，即“依照本法规定在合理的范围内处理已公开的个人信息”。因此，与 2020 年规范第 5.6(f)条项下没有“合理性”概念相比，本条件是有限定性的。虽然将第十三条第五项与第二十八条一并阅读表明，处理和个人信息最初发布的原始目的之间必须存在关系，但从第十三条第五项的起草中并未明确这一点。

与对于个人信息保护法（草案一次审议稿）一样，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[7]。

与对于个人信息保护法（草案一次审议稿）一样，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）。 此外，请参阅我们对第十四条关于间接获取个人信息的建议。 **(b) 删除“合理性”限定词** 我们建议，与2020年规范（其中包含受到金融机构欢迎的处理依据）保持一致，从利用数字工具高效开展关键职能以实现反洗钱合规和提高客户满意度的角度出发，从第十三条第五项中删除“合理性”概念。但是，如果法工委认为这一概念对于保护个人利益是必要的，那么金融机构和其他企业就有必要更好地理解对他们是不是“合理”处理的限定条件的期望到底是什么。
14	We note that any consent for processing personal information must be given “explicitly” (明确), 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 term “explicitly” 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 Second Review PIPL, “separate consent” is also referred to 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, if the nature of the consent required in each instance is not entirely clear (for example, explicit consent, deemed, voluntary consent, etc.), this will result in operational challenges for financial institutions to implement the law.	We recommend as follows so that financial institutions can better understand how to satisfy these fundamental requirements under the PIPL in practice, as their worries on operational uncertainty remain from the First Review PIPL: **(a) Meaning of “explicit” consent** We suggest clarifying the meaning of consent being given “explicitly”, and the nature of the consents needed more generally in each case in which the term is used. **(b) Meaning of “separate” consent** We suggest removing the concept of the “separate consent”, because: (i) it may be impractical to obtain in a digital context, depending on how it is defined; (ii) it could add to operational costs to administer collection, costs that would ultimately be passed on the customers of financial institutions and other business operators; and (iii) it would impact the user’s experience. We believe that, if needed, a notification obligation would be a

	We also note that the Second Review 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 individuals are ideally informed of the circumstances surrounding the collection and processing of their personal information.	sufficient alternative to a separate consent. However, if the Commission believes the requirement for a separate consent must be retained, we would suggest clarifying the meaning of "separate consent" to ensure compliance can be fulfilled by businesses from an operational perspective. **(c) Indirect collection of personal information** We suggest stating explicitly the viability of consent obtained by the original acquiror of personal information being relied on where the information is subsequently obtained indirectly by the personal information 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 the 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".
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。	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，因为它们仍然担心个人信息保护法（草案一次审议稿）中就存在的操作层面不确定性问题： **(a) "明确"同意的含义** 我们建议清楚说明"明确"同意的含义以及在被使用的每一种情况下，更为普遍需要的同意的性质。 **(b) "单独"同意的含义**

	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（草案二次审议稿）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，如果各种情况下所要求的同意（例如，明确同意、视为同意、自愿同意等）性质并不完全明确，将会导致金融机构在操作层面上面临实施法律的困难。 我们还注意到，个人信息保护法（草案二次审议稿）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。	我们建议删除“单独同意”的概念，因为： （i）取决于定义的不同，在数字环境下取得可能不切实际； （ii）可能将增加管理收集同意的运营成本，该成本将最终转移给金融机构和其他业务运营商的客户；及 （iii）将会影响用户体验。 我们认为，如果需要，通知义务足以代替单独同意。但是，如果法工委认为必须保留单独同意的要求，我们建议清楚说明“单独同意”的含义以确保企业可以从操作的角度符合要求。 **(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随后间接获取信息，可以依赖个人信息原有取得者取得的同意的有效性。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。
16	This article in the Second Review PIPL introduces the obligation for organisations to provide a “convenient means” for data subjects to withdraw consent.	While this is a common principle under other data protection regimes, financial institutions would require further guidance on what is expected to meet this standard of “convenience” in practice.
第十六条	在个人信息保护法（草案二次审议稿）中，本条规定组织有义务为数字主体撤回同意提供“便捷的方式”。	虽然这是其他数据保护制度下的常见原则，但金融机构需要获得进一步指导以了解在实践中其被期待采取哪些行动才符合“便捷”的标准。
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	We recommend that the obligation to continue the provision of products or services under this article should only apply where the personal information

	information, except where the processing of personal information is necessary for the provision of products or services.	that the organisation seeks to collect and process is not within the reasonable (objective) expectation of the individuals concerned. This would not be out of line with rules released since the First Review PIPL (such as Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications (《常见类型移动互联网应用程序必要个人信息范围规定》) on the categories of personal information that regulators assert are objectively necessary for the operation of certain mobile applications. 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。这在监管机构认定为操作某些移动应用程序所客观必需的个人信息种类方面，不会违反自个人信息保护法（草案一次审议稿）以来所发布的规则（例如，《常见类型移动互联网应用程序必要个人信息范围规定》）。 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 this 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。
21	This article states that personal information processors hold joint and several liability when they jointly process personal information. However, it is not clear in the event of certain mandatory obligations (such as data breach reporting as required under Article 56) which personal information processor should bear the liability (in this case of notifying the competent regulator as well as the data subject of a data breach).	We recommend clarifying more fully the expectations on joint processors to better facilitate cooperation between financial institutions and business partners (as well as other organisations) to foster the digital economy more efficiently. In particular, the Commission should consider clarifying how joint responsibilities of personal information processors relate to scenarios where one personal information processor indirectly acquires personal information via the other personal information processor, for which a different set of obligations is already suggested under Article 5.4(e) of the 2020 Specification.
第二十一条	本条规定，多家个人信息处理者共同处理个人信息时，应当承担连带责任。但是，不清楚对于某些强制性义务（例如，第五十六条要求的数字侵权报告），应由哪一家个人信息处理者承担责任（在前述例子的情况下，须通知主管监管部门和遭遇数字侵权的数字主体）。	我们建议更为全面地澄清对共同处理者的期待以更好地促进金融机构和商业合作伙伴（以及其他组织）的合作，从而更高效地培育数字经济。特别是，法工委应考虑澄清，在一家个人信息处理者通过另一家个人信息处理者间接获取个人信息的情况下（对此，2020 年规范第 5.4(e)条已经建议了一套不同的义务），个人信息处理者如何承担连带责任。
22	**(a) Vague definitions of key players** 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 “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	**(a) Differentiation of concepts of “controller” and “processor”** 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, as Article 58 does not elaborate on liabilities apportionment. **(c) Clarify retention requirements**

	clear definition concept of "processor" is omitted. **(b) Entrusted party obligations** 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, notwithstanding the introduction in the Second Review PIPL of Article 58 on entrusted parties' responsibilities. **(c) Retention of data** The Second Review PIPL clarifies that an entrusted party must not retain personal information after its entrustment contract is terminated, revoked or found to be invalid. Although this is not a substantive change to the obligations on entrusted parties, there are clearly more responsibilities imposed on these processors under the Second Review PIPL compared to existing data protection laws (for example, the responsibilities imposed on entrusting parties under Article 58).	Service providers to financial institutions may be concerned by the increased obligations on them to handle data appropriately. In addition, where entrusted parties have no contractual terms in place with the personal information processor but there is a statutory requirement on them to retain personal information, they should be provided with a reasonable period of time in which to expunge the personal information or a clear exception to the requirement to expunge that information (as is the case for personal information processors under Article 47).
第二十二条	**(a) 关键参与者的概念模糊** 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。 **(b) 受托方义务**	**(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，因为第五十八条并未阐明责任分担事宜。 **(c) 说明数据保留要求** 金融机构的服务提供方可能担忧他们有了必须适当处理数据的更多义务。此外，如果受托方与个人信息处理者之间没有合同条款，但有关于让该受

	虽然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，尽管个人信息保护法（草案二次审议稿）第五十八条介绍了受托方的责任。 **(c) 保留数据** 个人信息保护法（草案二次审议稿）明确说明了，委托合同不生效、无效、被撤销或者终止后，受托方不得保留个人信息。虽然未对受托方责任作出实质性变更，但较现行数据保护法而言，这些处理者在个人信息保护法（草案二次审议稿）项下承担的责任明显更多（例如第五十八条中关于委托方的责任）。	托方保留个人信息的法定要求，则应为他们提供合理的时间以清除个人信息或明确规定删除该信息要求的例外情况（同第四十七条项下个人信息处理者的情况相同）。
24	**(a) Separate consent for transfers to other parties** Separate consent is required from individuals where a personal information processor engages another party to process the personal information. However, in such circumstances, there may be other legal bases for processing personal information. The Second Review PIPL seems to clarify that the other legal bases for a processor to process personal information under Article 13 apart from consent would override the requirement for any consent (separate or otherwise) in other articles of the PIPL, but this remains ambiguous. 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. However, the change in terms between the First Review PIPL (which used "third party") and the Second Review PIPL	**(a) Reduce (if not remove) separate consent requirements** We suggest specifying explicitly that the disclosure of personal information to other parties is permitted if any of the processing grounds established under Article 13 (other than the consent of the individual) is met. This is a crucial operational point for financial institutions that remains from the First Review PIPL. 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". For financial institutions which implement robust outsourcing governance practices and other data transfer protocols, existing mitigating controls already exist. Indeed, the

	(which uses "other party") seems to emphasise that this requirement applies to all transfers to other persons. **(b) Notification requirements** It would not be practicable to notify individuals of the identity of each 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.	sharing of customer information within a corporate group is an approach that is advocated by international financial services organisations (such as the Financial Action Task Force[8]) and domestic bodies (such as the CBIRC[9]) to strengthen AML/CFT processes. Especially where affiliated entities are wholly owned by the same holding company, the transfer of information to such an affiliate should not result in a tangible increase in risk for data subjects. In addition, multiple entities in the same group may be providing one customer different services or products given the need often for separate regulatory licences, so sharing personal information without additional consents is beneficial from the perspective of the customer's experience. **(b) Narrow notification requirements** We recommend that individuals be notified of the categories (instead of the exact identities) of recipient of their personal data. This is consistent with international norms, including GDPR (Article 13.1(e)) and also avoids requiring a financial institution to disclose an existing business relationship that might amount to commercial value in itself. If the notification requirements are not narrowed despite the commercial and practical issues, it will be imperative for financial institutions to receive further guidance as to the level of information that is expected to be provided on data recipients and the

[8] Article 18 of The FATF Recommendations as amended in 2020.
2020 年修订的《反洗钱金融行动特别工作组建议》第 18 条。

[9] Article 19 of the Guiding Opinions of the General Office of the China Banking and Insurance Regulatory Commission on Strengthening the Development of a Long-Term Compliance Management Mechanism for Overseas Agencies of Chinese-Funded Commercial Banks.
《中国银保监会办公厅关于加强中资商业银行境外机构合规管理长效机制建设的指导意见》第 19 条。

		method of providing that information to data subjects. **(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.
第二十四条	**(a) 向他人提供信息须取得单独同意** 个人信息处理者委托他人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。个人信息保护法（草案二次审议稿）第十三条似乎在澄清关于处理者处理个人信息的除同意以外的另一个法律依据，这项法律依据将超越个人信息保护法其他条款中的任何同意（单独或其他同意）的要求，但这个意思不太清晰。 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。但是，个人信息保护法（草案一次审议稿）（采用“第三方”的说法）和个人信息保护法（草案二次审议稿）（采用“他人”的说法）之间的变动似乎强调，此项要求适用于向其他人士进行的任何转移。 **(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	**(a) 降低（若非删除）单独同意要求** 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，即可向他人披露个人信息。对于金融机构而言，这是个人信息保护法（草案一次审议稿）遗留的一个关键点。 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”。对于实施良好外包治理和其他数据转移协议的金融机构，现有降低控制的要求已经存在。确实，在公司集团内部共享客户信息是国际金融服务组织（比如金融行动特别工作组[8]）和国内机构（比如银保监会[9]）倡导的措施，以增强反洗钱反恐融资流程。尤其是，如果关联实体由同一控股公司全资拥有，向该关联方转移信息应当不会实质增加数据主体的风险。此外，因为通常需要单独的监管许可，同一集团内部的多家实体可向一家客户提供不同服务或产品，因此从客户体验角度

	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。	而言，在无需同意的情况下共享客户信息将有所裨益。 **(b) 降低告知要求** 我们建议向个人告知个人数据接收人所属类别，而非确切身份。这与国际规范一致，包括 GDPR（第 13.1(e)条），并且可避免要求金融机构披露可能对其有商业价值的现有商业关系。 尽管存在商业和实践因素，但如果仍未对告知要求有所限缩，必须对金融机构应向数据接收方提供之信息的级别以及如何向数据主体提供该信息的方法有所指导。 **(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。
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 result" to be guaranteed. This is problematic owing to the black-box uncertainty and "un-explainability" that is inherent in 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".	We recommend that such guarantees be provided only if use of ADM "produces legal effects concerning the individual or similarly significantly affects the individual" and where no method other than ADM is used to produce the outcome. For the obligation to explain ADM processing and the required opt-out for data subjects, while we note the change from the First Review PIPL clarifies that these rights are triggered on the objective basis that the resulting decisions have a material impact on an individual's rights and interests, we continue to recommend clarifying what would constitute "material impact on their rights and interests". Further, we propose to include 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) it is 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"结果公平合理"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"对个人产生法律效力或类似的重大影响"以及除通过自动化决策以外无任何其他方法产生此等效果的情况下提供该等保证。 关于与要求说明通过自动化决策作出决定相关的义务以及必须为数据主体提供退出选项的义务，虽然我们注意到，个人信息保护法（草案一次审议稿）修改后，明确规定，这些权利是因形成的决定对个人权益客观上存在实质性影响，但我们仍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 the concept of "disclosing" under this Article is intended to entail. This Article addresses separate consent for the disclosure of personal information.	We recommend clarifying the concept of "disclosure" under this Article to include, as seen in the 2020 Specification, 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. Requiring maintenance of multiple consents will create additional concerns. However, if the new text in Article 13 seeks to clarify that consent under Article 26 is not required in the case that one of the other processing grounds under Article 13 is present, we suggest specifying explicitly in Article 26 that

		that is the intent of the revisions to Article 13 in the Second Review PIPL.
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，以包括将个人信息处理者向关联实体披露这种例外（如同2020年规范中那样）。 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难。我们建议在收集*或*披露时获取同意。要求维护多个同意会产生其他问题。但是，如果第十三条的新规定试图说明，若存在第十三条下的任何其他处理依据，则不再要求第二十六条项下的同意，则我们建议，在第二十六条中明确说明这是个人信息保护法（草案二次审议稿）修改第十三条的初衷。
27	We note that the Second Review PIPL narrows the circumstances in which personal images and personal identity and attributes information can be disclosed to only where the relevant individual gives a separate consent. The reference to “or as provided by laws or administrative regulations” has been removed from the provision in the First Review PIPL. Following this change, it is unclear whether financial institutions that install image collection or other identity recognition equipment remain permitted to provide personal images, identity and attributes information to public security agencies. However, the Second Review DSL introduces additional penalties in instances where organisations or individuals do not cooperate with public and national security authorities in providing access to data.	We suggest that the PIPL or DSL clarifies the obligations on financial institutions and other organisations in respect of providing this type of information to public and national security authorities, particularly in light of the newly proposed sanctions should there be an instance of non-compliance.
第二十七条	我们注意到，个人信息保护法（草案二次审议稿）将可以披露个人图像和个人身份识别及特征信息的情况限缩至仅仅当相关个人给予单独同意时。个人信息保护法（草案一次审议稿）中“或者法律、行政法规另有规定的除外”的表述已被删除。变更后，安装图像采集或其他身份识别设备的金融机构是否仍被允许向公共安全机构提供个人图像和个人身份识别及特征信	我们建议，个人信息保护法或数据安全法说明，金融机构和其他组织在向公共和国家安全机构提供此类信息时的义务，尤其是针对任何未遵守规定的情况的拟议制裁。

	息，尚不明确。但是，数据安全法（草案二次审议稿）增加了组织或个人未配合公共或国家安全机构提供数据时将遭受的额外处罚。	
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 and innovation being a central tenet of "Digital China" under the 14th Five Year Plan, 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 the meaning of "reasonable scope" is, 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 or 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	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。

	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（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且创新成为十四五计划下“数字中国”的核心宗旨的背景下，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。	我们建议明确“合理范围”的含义或定义，例如通过明确提述 2020 年规范第 7.3(a)条（如适用）。
29	As in the First Review PIPL, 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	与个人信息保护法（草案一次审议稿）相同，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. Requiring 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 5.4(e) of the 2020 Specification. We would also urge an exception be provided where processing sensitive personal information is required by law and to protect vital interests. If the new text in Article 13 seeks to clarify that separate consent under Article 30 is not required in the case that one of the other processing grounds under Article 13 is present, we suggest specifying explicitly in Article 30 that that is the intention of the revisions to Article 13 in the Second Review PIPL.
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。维护多项同意也将产生额外问题。 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。如果第十三条的新规定试图说明，若存在第十三条下的任何其他处理依据，则不再要求第三十条项下的同意，则我们建议，在第三十条中明确说明这是个人信息保护法（草案二次审议稿）修改第十三条的初衷。
Chapter III Rules on Cross-Border Provision of Personal Information **第三章 个人信息跨境提供的规则**		
38	**(a) Lack of clarity on security assessment and certification requirements** It remains unclear from the First Review PIPL whether the security assessment under item 1 of Article 38 and the certification under item 2 of Article 38 constitute one-time	As for the First Review PIPL, 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

	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 remain hugely concerned that requiring assessments/certifications for each and every transfer is 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.	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. Foreign-invested financial institutions operating in the PRC have long track-records of transferring client information in a secure manner on a cross-border basis, and would relish an opportunity to discuss proposals with the Commission and competent departments with an aim to ensure that the scope and detail of assessments is proportionate to the actual risk (if any) of harm and giving proper regard to accountability. We would urge industry engagement on any sectoral requirements for security assessments to ensure specific requirements for financial services are incorporated in harmony with existing regulatory requirements and allow financial institutions to apply a risk-based approach and update risk management frameworks accordingly. If a security assessment or certification requirement is to remain, we continue to urge an exception for intra-group transfers to facilitate efficient business operation. See our similar comments in respect of Article 24. 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 尚不清楚个人信息保护法（草案一次审议稿）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，我们仍然非常担心，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。	关于个人信息保护法（草案一次审议稿），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。在中国境内开展业务的外资金融机构拥有长期的跨境安全转移客户信息的良好记录，并非常希望能够有机会与法工委和主管部门商讨各种方案，以确保相关评估的范围和细节与实际的损害风险（如有）在程度上相适应，并考虑相应的问责情形。 我们促请相关行业人员参与对安全评估相关要求的制定，以确保金融服务行业的特定要求与现有监管要求相协调，并允许金融机构采纳以风险为导向的方式并对其风险管理框架进行相应的更新。 如果保留安全评估或认证要求，我们继续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 the PRC by concluding a contract with the foreign recipient.	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 existing or newly implemented contractual terms

	However, the PIPL does not provide any details on the necessary contractual terms, except that (as stated in the Second Review PIPL) the CAC shall provide a standard contract at some later time.	that conform to international standards (such as the GDPR's standard contractual clauses) or otherwise provide equivalent protection to the contractual terms. If, however, mandated contractual terms will have a more comprehensive scope than typical international standards in this regard, we would also suggest that the Commission expressly recognises and distinguishes between foreign recipients that are personal information processors (or "data controllers") as opposed to entrusted parties (or "data processors"). Alternatively, the CAC could provide a general description of the contractual terms that are required within contractual frameworks formulated by organisations, with the standard contract constituting only a guidance document. This approach would be in line with the data protection regimes of other financial centres in Asia.[10] In addition, we suggest restoring and supplementing item 3 of Article 38 as follows: *"Having concluded a contract with the foreign receiving party ~~based on the standards contract prepared by the State cyberspace authorities~~, agreeing on both sides' rights and obligations, and supervising their personal information processing to ensure that the personal information protection standards provided under this law are met. State cyberspace authorities will prepare a standard contract template which shall serve as*

[10] For example, Article 26 of the Personal Information Protection Act of South Korea together with Article 28 of the Enforcement Decree of the Personal Information Protection Act of South Korea and NPC Circular No. 2020-03 on Data Sharing Agreements of the Philippines follow such an approach. Likewise, the guidance on cross-border data transfers published by the Privacy Commissioner for Personal Data in the Hong Kong Special Administrative Region also adopts a recommended instead of mandatory adoption approach.

举例而言，韩国《个人信息保护法》第 26 条及韩国《个人信息保护法执行法令》以及菲律宾国家隐私委员会关于数据分享协议的第 2020-03 号通知均采用此方法。

		reference for personal information processors." The CAC should also publish a timetable for release and implementation of these contractual terms or other guidelines, as these will be crucial for financial institutions' operational implementation planning before launch of the PIPL. We urge the Commission to consider that there is a transition period of at least 24 months following the date on which the PIPL or (if released later) the relevant implementing rules setting out the requirements for these contractual terms come into force. Opportunity should also be given to financial institutions and other businesses to provide feedback on the proposed standard contractual clauses considering the importance of these clauses to facilitating cross-border business.
	(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。虽然个人信息保护法并未就必要的合同条款作出具体规定，但正如个人信息保护法（草案二次审议稿）所述，国信办将会制定该等标准合同。	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现有或新实施的合同条款（例如 GDPR 的标准合同条款）或为其合同条款提供同等的保障。 但是，如果强制性合同条款在此方面的范围较典型的国际标准更为全面，我们也建议法工委对本身是个人信息处理者的境外接收者（"数据控制者"）与受托方（"数据处理者"）进行明确的确认及区分。 或者，国信办可就各组织制定的合同框架内要求的合同条款提供一个概述性说明，而标准合同则仅作为一个指南性质的文件。该等方法也与亚洲其他金融中心的数据保护制度相一致。[10] 此外，我们建议恢复第三十八条第（三）项如下： "*~~按照国家网信部门制定的标准合同~~与境外接收方订立合同，约定双方的权利和义务，并监督其个人信息处理活*

		动达到本法规定的个人信息保护标准。国家网信部门将制定一个标准合同模板，供个人信息处理者参考。” 国信办还应就发布和实施该等合同条款或其他指引公布一个时间表，因为在个人信息保护法出台之前，该等条款或指引对金融机构的运营实施规划至关重要。我们促请法工委考虑提供至少 24 个月的过渡期，从个人信息保护法生效之日或载明该等合同条款要求的相关实施细则生效之日（以较后者为准）起算。鉴于拟议标准合同条款对促进跨境业务的重要性，还应为金融机构和其他企业提供机会，使其能够就拟实施的标准合同条款提供反馈意见。
	(c) Affiliate exemption We note that the restriction under Article 38 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 under the PIPL. However, if the Commission believes that the requirement for a security assessment must be retained in this instance, we would suggest that a risk-based approach is taken such that a security assessment is only required where the sharing, disclosure or transfer of personal information gives rise to a material change in the purpose or manner of the data processing. To align with international banking practice, we recommend that transfers of personal information to outsourced service providers, which process the information under the direction and responsibility of the onshore financial institution, should be similarly exempt from any security assessment under the PIPL. This would be on the basis that the transferor would take responsibility for such entrusted party’s obligations relating to the personal information processing activities carried out on behalf of the transferor.

	(c) 关联方豁免 我们注意到，第三十八条下的限制范围十分宽泛，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，则无需进行个人信息保护法下的任何安全评估。但如果法工委认为在这种情况下必须保留进行安全评估的要求，那么我们建议采用以风险为导向的方式，只有在共享、披露和传输个人信息会对数据处理的目的或方式产生实质变更的情况下才进行安全评估。 为了与国际银行业惯例保持一致，我们建议将个人信息传输给外包服务提供商的行为（外包服务提供商在境内金融机构的指导和承担责任的基础上处理信息）应同样获豁免进行个人信息保护法下的任何安全评估。这也是由转让方来承担与委托方有关代表转让方进行的个人信息处理活动的义务的基础。
	(d) Other exemptions In digital economies where transnational business promotes trade and improved service offerings, it is common for the market to provide other transfer mechanisms to facilitate legal and secure cross-border transfers of personal information. The options available under the PIPL arguably lack diversity to promote efficient business operations for the benefit of individuals within the PRC.	As for the First Review PIPL, we recommend that other options should be included to facilitate overseas transfers (without separate consent – see our comments on Article 39 below). Options to be considered include binding corporate rules for intra-group transfers, model contracts and certification schemes including the APEC CBPR as noted in our comments to Article 12, or other circumstances where the recipient of the transferred personal information provides a standard of protection that is at least comparable to the protection under the PIPL. In addition, where an individual voluntarily sends his or her personal information to an overseas recipient (such as an offshore financial services provider for the provision of cross-border banking services) or instructs an onshore financial institution to do so on his or her behalf, this should be stated to be outside the restrictions on data exports under this Chapter III.
	(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，由市场来提供其他转移机制，以便个人信息合法且安全地	对于个人信息保护法（草案一次审议稿），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）。其他选择包括关于集团内部传

	出境是常见的。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。	输的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）以及由个人信息传输的接收方提供一个至少与个人信息保护法下的保护相当的标准。此外，如果个人自愿将其个人信息发给境外接收方（例如提供跨境银行服务的境外金融服务提供商）或指示某境内金融机构来进行，该等行为应当被明确不在本第三章项下数据跨境提供的限制范围内。
39	**(a) Notification and consent requirements** If the personal information of a data subject is to 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, as noted in our comments on Article 14, requiring individual consent for every situation will place unnecessary burdens on the individual and may result in "consent fatigue" without furthering the individual's privacy rights. Furthermore, Article 39 requires personal information processors to explain the ways for data subjects to exercise their individual rights over a recipient of personal information located outside the PRC. However, there would not be a direct contractual relationship between the data subject and the foreign recipient, so enforcing such rights against foreign recipients	**(a) Clarifying notification and consent requirements** Please see our comments on Article 14 on 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 (unless it is already the intention of the new text in Article 13 of the Second Review PIPL to clarify this to be the case); and (2) only the categories/types of third-party recipients should be notified to individuals. As for the First Review PIPL, 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 *category/type* of third-party recipient. The interests of data subjects ought to be assessed and balanced against the practical

	would involve complex cross-jurisdictional issues. **(c) Indirect acquisition of personal information** Where the client of a financial institution is an institutional rather than an individual client, it is technically not the data subject's consent that should be required to collect and process any personal information, for instance for anti-money laundering / know-your-customer purposes (e.g. details of the legal representative, directors, etc.). The market practice is for financial institutions in the PRC to seek contractual confirmations from their institutional clients that they have obtained prior consent from their representatives to provide their data to the financial institutions, as it is impractical for the financial institutions 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.	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. Indeed, given the overlap between the requirements set out in Article 24 and Article 39 in respect of transfers to third parties, the Commission may consider whether Article 39 may be deleted in its entirety (Article 38 then being relied on in respect of any additional requirements for personal information to be transferred on a cross-border basis). **(b) Responsibility for addressing data subject rights** In addition, we would recommend that the Commission is consistent with the approach taken under Article 9.2(h) of the 2020 Specification, which stipulates that personal information controllers should "help the PI Subjects to understand … the rights of the PI Subjects, such as the right to access, rectify, delete information and to de-register", without suggesting that there is a direct right of recourse to the foreign recipient. Rather, the onshore transferor of the personal information would, in practice, seem a more logical party for the data subject to contact – not least as it is the transferor which shall "bear the corresponding responsibility for any damage on the legitimate rights and interests of the PI Subjects incurred by security incidents due to the sharing and transfer of PI" (pursuant to Article 9.2(g) of the 2020 Specification).

		That said, in support of inclusion of an affiliate exemption, any recourse to an overseas recipient would be unnecessary where the receiving party is in the same corporate group and the individual can exercise his or her rights through the onshore transferring party. **(c) Explicit reference to indirect acquisition** We also recommend specifying whether the indirect acquisition of personal information is recognised under the requirements of the PIPL. **(d) Local copy requirement** We suggest clarifying whether retaining a local copy of the personal information transferred overseas is also generally required under the PIPL and other related laws.
第三十九条	**(a) 通知和同意要求** 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，根据我们对第十四条提出的意见，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。 此外，第三十九条要求个人信息处理者应当向个人告知向境外的个人信息接收方行使其权利的方式。但是，由于该等个人与境外接收方之间将不存在直接的合同关系，因此，对境外接收方主张该等权利将会在执行层面涉及复杂的跨司法辖区的问题。 **(b) 个人信息的间接获取**	**(a) 澄清通知和同意要求** 请参见我们对第十四条提出的意见，即澄清“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（除非个人信息保护法（草案二次审议稿）第十三条的新增文字已旨在澄清这一点）；以及（2）仅向个人告知第三方接收者所属范畴/类别。 关于个人信息保护法（草案一次审议稿），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

	在金融机构的客户是机构客户而非个人客户的情况下，在技术上，收集和处理任何个人信息时，必须征求的不是数据主体的同意，比如出于反洗钱/了解您的客户的目的（比如法定代表人、董事等的详细信息），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以合同的方式确认其已取得相应机构客户代表的事先同意，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。	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。确实，鉴于第二十四条和第三十九条所述的关于向第三方传输的要求之间有重叠，法工委可考虑是否可将第三十九条整体删除（由此，关于对跨境传输个人信息的任何额外要求则依赖第三十八条）。 **(b) 处理数据主体权利的责任** 此外，我们还建议法工委延续 2020 年规范第 9.2(h)条项下的处理方式，该条规定，个人信息控制者应当“帮助个人信息主体了解……个人信息主体的权利，例如，访问、更正、删除、注销账户等”，但没有暗示存在对境外接收方的直接追索权。相反，在实践中，对个人信息主体而言，个人信息的境内传输方似乎是更符合逻辑的联系人 – 至少是“因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的”，传输方“应承担相应的责任”（根据 2020 年规范第 9.2(g)条的规定）。 就此，考虑到增加关联方豁免的建议，在接收方同属一公司集团而且个人可通过境内传输方行使其权利的情况下，无需对境外接收方的实施任何追索。 **(c) 对间接获取的明确引用** 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。 **(d) 当地副本要求** 我们建议澄清，个人信息保护法及其他相关法律是否普遍要求在当地留存出境个人信息的副本。
40	**(a) Reconsideration of the localisation requirement** We assert, as in our submission on the First Review PIPL, that the proposed requirements around data localisation in Article 40 should be reconsidered, as localisation of personal information does not serve to effectively improve protection of individuals' rights and interests. In	We strongly suggest removing the requirement to store personal information only in the PRC. Instead, new arrangements should be established to protect data transferred offshore in accordance with the security requirements that would otherwise apply to the information onshore.

	contrast, requirements mandating personal information to be retained onshore or subject 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, risk management controls and business continuity. The restrictions serve to reduce product and service offerings, and impair the quality of any offerings, to Chinese customers, 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 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.	Alternatively, if a localisation requirement must be retained, we suggest at least: • clarifying that any security assessment should be formulated and conducted by the relevant industry regulator (or, in the absence of an appropriate industry regulator, the competent provincial authority) since the CAC will unlikely have the resources to cover nationwide assessments or the granular knowledge of the industry in question to be an effective regulatory body for these purposes; • permitting back-up copies of data to be retained outside the PRC for business continuity, subject to compliance with applicable data security requirements; and • 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 based on quantum of personal information involved is not in line with international norms.
	(a) 重新考虑本地化要求 正如我们就个人信息保护法（草案一次审议稿）提出的反馈意见，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、风险管理控制和业务持续性的效	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，应作出新的安排根据适用于境内信息传输的安全要求对向境外传输的数据提供保护。 或者，如果必须保留本地化要求，我们建议至少： • 澄清任何安全评估应由相关行业监管机构（如没有适当的行业监管机构，则由具有管辖权的省级机关）制定并进行，因为国信办

	果。该等限制性规定将降低向中国消费者提供的产品和服务的数量与质量，最终对中国在国际贸易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。	将不大可能拥有资源覆盖全国范围的评估，也不大可能拥有相关行业的详细知识，以作为一个有效的监管机构来实现这些目标； • 允许为了业务持续性的目的在境外保留数据备份，但需遵守适用的数据安全要求；以及 • 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。
	(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 the 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 and implementation of the 2017 Draft CII Measures or other measures which will set out an unambiguous term. We suggest the relevant sector regulators actively seek the views of market participants and involve them in the process of formulating the 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 coordinating regulator for financial institutions in respect of Article 59.
	(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和实施时间表。 我们建议有关行业监管者积极征求市场参与者的意见，邀请其参与关键信息基础设施定义以及特定行业的任何相关要求的制定流程。同时请参阅我们就第五十九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。

	(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.	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）。	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 remains extremely broad in the Second Review PIPL. 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 个人信息保护法（草案二次审议稿）中第四十条的适用范围仍然非常宽泛。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. 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	As in our submission for the First Review PIPL, we strongly recommend expressly clarifying that this article does not apply: (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

	enforcement bodies and, pursuant to the Second Review PIPL, judicial bodies, similar to the obligation in respect of data under Article 35 of the DSL. In addition, we note in the Second Review PIPL that the right for provision of personal information in accordance with international mutual assistance treaties and similar agreements to which the PRC is a party no longer expressly prevails over the PIPL restrictions. We continue to submit that this expansion will create major issues for global financial institutions headquartered outside 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.	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 AML and CFT purposes; (d) to provision of personal information to international organisations (e.g. Interpol), re-instating the exception from the First Review PIPL allowing organisations to observe international mutual assistance treaties and similar agreements to which the PRC is a party; or (e) to provision of personal information to foreign government authorities as required by the applicable local laws, with only a very narrow scope of foreign authorities or other bodies (if any) that are barred in explicitly defined circumstances from receiving personal information. We also ask that the meaning of "foreign law enforcement bodies" be clarified: in particular, whether financial regulators, tax bureaux, exchanges and clearing houses will be considered "foreign law enforcement bodies". 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).

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，与数据安全法第三十五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以及个人信息保护法（草案二次审议稿）中提及的司法机构要求提供的在中国存储的个人信息。 此外，我们注意到在个人信息保护法（草案二次审议稿）中，根据中国缔结或者参加的国际条约、协定提供个人信息的权利不再明确优先于个人信息保护法中的限制。 我们还认为，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。	正如我们就个人信息保护法（草案一次审议稿）提出的反馈意见，我们强烈建议明确说明本条不适用于下列情况： (a) 不太可能危害国家安全或公共利益的个人信息。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，重新采纳个人信息保护法（草案一次审议稿）中允许各组织遵守中国缔结或者参加的国际条约、协定的优先适用的表述；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，并只有极小范围的外国机构或其他机构（如有）在明确规定的情况下会被禁止接收个人信息。 我们还建议明确“境外的执法机构”的含义：特别是，金融监管机构、税务局、交易所和清算所是否会被认为是“境外的执法机构”。 我们建议，相关主管机构同步修改现行的类似限制（例如，证监会禁止在未经其批准的情况下分享“与证券业务活动有关的数据”、中国银保监会限制向离岸供应商传送客户资料（不论是否已加密））。
42	A key concern of this Article is its extraterritoriality, which we believe should be limited to the maximum extent possible in respect of supervising harm to “the national security or public interest of the People’s Republic of China”. This overlaps with the powers provided under the DSL, which continues with the Second Review DSL to be the	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 the PRC. Overlaps with any existing law –

	better law to deal 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 extraterritorial 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.	as well as the forthcoming DSL – 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 the PRC in order to be subject to any investigation or enforcement. In addition, since the First Review PIPL, our membership has further emphasised that the implementing rules of the GDPR should be noted as further discussing how extraterritoriality is aimed only at an intentional, targeted offering of goods or services to individuals in the EU, as opposed to where the provision of goods or services is incidental or inadvertent. As for the First Review PIPL, we urge that the PIPL must prescribe similar indications to those in the GDPR as to the extent of its extraterritorial application on the offering of goods or services.
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	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

	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，而数据安全法（草案二次审议稿）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。	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以及即将出台的数据安全法重叠。 我们促请个人信息保护法应围绕中国境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。 此外，自个人信息保护法（草案一次审议稿）以来，我们的成员已经进一步强调指出，在进一步讨论如何将域外法权仅针对有意的、有针对性地向欧盟个人提供商品或服务，而不是偶然或无意的提供商品或服务时，应留意 GDPR 的实施规则。同个人信息保护法（草案一次审议稿）一样，我们促请个人信息保护法在涉及提供商品或服务方面适用域外法权的范围应当作出与 GDPR 类似的规定。
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 for supervising

		compliance with 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”； (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 50. Limitations to individuals' rights may be necessary, for reasons such as (but not limited to) protecting the public interest, protecting the rights of other individuals and other legitimate reasons. Article 50 of the Second Review PIPL 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 during legal proceedings[11]. 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五十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。个人信息保护法（草案二次审议稿）第五十条规定拒绝个人行使权利的请	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，或在诉讼程序期间[12]。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。

[11] Both the GDPR and Hong Kong Personal Data (Privacy) Ordinance introduce qualifications to the access rights of data subjects in certain circumstances (for example, under section 20 and the exemption provisions under Part 8 including sections 54(1), 55, 58(1), 60 and 60A of the Personal Data (Privacy) Ordinance).

[12] GDPR 和香港《个人资料（私隐）条例》在某些情况下对数据主体的访问权引入限制条件（例如：《个人资料（私隐）条例》第 20 条下的规定以及第 8 部下的豁免条款（包括第 54(1)、55、58(1)、60 和 60A 条））。

	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。	
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 "know-your-customer" for 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 requires personal information processors to cease processing of personal information when technical difficulties are encountered in the processing and deletion of personal information.	**(a) Clarification on Article 47(3)** We recommend clarifying that the obligation to delete personal information should only apply when a processor processes personal information based on consent obtained from the individual (and not any other processing ground in Article 13). We also recommend that such deletion should not be required where it would contradict a legal obligation on the personal information processor or the existence of another legitimate interest (such as handling future disputes). A similar provision is set out under the Article 17.1(b) of the GDPR. **(b) Clarification on technical difficulties** We recommend further clarifying what may constitute technical difficulty in this respect (examples or scenarios being welcomed).
第四十七条	**(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（而非第十三条中的任何其他依据），才有义务删除相关个人信息。我们还建议，如果与个人信息处理者的法律义务或存在的其他合法权益（例如处理将来的争议）相抵触，则不应该要求该等删除。GDPR 第 17.1（b）条规定了类似的限制条件。 **(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）。
49	The rights of individuals under Chapter 4 of the PIPL are extended in the Second Review PIPL to deceased individuals. These rights may be exercised by the deceased's close relatives. However, no details are provided under the Second Review	**(a) Clarification on scope of "relatives"** We recommend that the Commission clarifies that "relatives" are those

	PIPL as to how these rights should be enforced by the close relatives in practice (such as what evidence of relationship or power of attorney must be provided by the relative) and therefore what financial institutions or other businesses will need to do to prepare for such requests from next of kin.	individuals set out in Article 1045 of the Civil Code, if that is the case. **(b) Guidance on exercise of rights** In addition, we suggest that guidance is prepared on how relatives exercise the rights of the deceased to enable financial institutions to adapt back-office processes accordingly.
第四十九条	个人信息保护法（草案二次审议稿）将第四章下的个人权利延伸至了已死亡的个人。相关权利可由其近亲属行使。但是个人信息保护法（草案二次审议稿）未就近亲属在实践中如何执行此项权利（例如亲属必须提供何种亲属关系证明或授权委托书），以及金融机构或其他企业因此需要采取何种措施来应对近亲属提出的此类请求作出详细规定。	**(a) 明确"亲属"的范围** 我们建议法工委明确说明"亲属"是指《民法典》第一千零四十五条下列明的个人（如果该条的本意即如此）。 **(b) 关于行使权力的指引** 此外，我们建议就亲属如何执行已死亡个人的权利提供指导意见，以便金融机构相应地调整其后台业务流程。
Chapter V Obligations of Personal Information Processors **第五章 个人信息处理者的义务**		
51	We submit that it is unclear under item (3) of Article 51 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. In addition, any overlap between this Article 51, Article 26 of the DSL and Article 11.1 of the 2020 Specification should be resolved.	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. We recommend that financial institutions should be permitted to adopt international encryption standards, or other encryption standards which are no less stringent than Chinese-formulated algorithms. More generally, similar requirements under the PIPL, DSL and 2020 Specification for appointment of a data protection officer should be reconciled to facilitate businesses in ensuring that accountability and responsibilities lie with the right individual/function. Similarly, we would recommend clarifying the responsibilities of these personal information management personnel under the PIPL compared to the role of the person in charge of cybersecurity under Article 21 of the CSL. See our further comments on Article 52 below.

第五十一条	我们认为，根据第五十一条第（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，应解决本第五十一条条与数据安全法第二十六条和 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。我们建议，金融机构应当获准采用国际加密标准或不比中国制定的算法宽松的其他加密标准。 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，有助于企业确保由正确的个人/职能部门承担责任。同样，我们也建议明确这些个人信息管理人员在个人信息保护法下的责任与在网络安全法第二十一条下负责网络安全人员的责任。请进一步参见下述我们对第 52 条的反馈意见。
52	**(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. As in the First Review PIPL, the threshold amount has not been specified in the Second Review PIPL.	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 is recommended that the mandatory threshold be set 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，但同个人信息保护法（草案一次审议稿）相同，个人信息保护法（草案二次审议稿）中并未明确数量门槛。	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	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 under the PIPL or, if more appropriately set out in other implementing rules or guidance, providing reference to such rules or

	PIPL and CSL can be met through the appointment of a single individual.	guidance (such as a further supplemented version of the 2020 Specification): • that the person in charge of personal information can share roles between group companies, affiliates 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.
	(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，我们建议在个人信息保护法下明确以下各项，或若在其他实施细则或指引中进行规定更为适合的话，提述其他指引（例如 2020 年规范）： • 个人信息保护负责人可同时承担集团各公司、关联方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。
53	PIPL requires an offshore processor that analyses or assesses 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 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.
第五十三条	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。
54	Article 54 imposes a compliance audit requirement on all personal information processors.	We recommend that the compliance audit requirements only be required where determined pursuant to a prescribed risk-based assessment of a financial institution's processes.
第五十四条	第五十四条对所有个人信息处理者施加了一项合规审计要求。	我们建议金融机构的合规审计应基于其以风险为导向得出的评估结果而决定是否进行。
55	Article 55 suggests a wide range of activities where risk assessment is required. We submit that some of these activities are "business as usual" operational activities. For example: • 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 only to 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	Please see the Financial Services Sector Cybersecurity Profile developed by the Financial Services Sector Coordinating Council[13] as an example of a risk-based assessment tool which may be a useful reference for the Commission. The Cybersecurity Profile can be further updated to include mapping of local efforts to support those operators within the PRC. We recommend taking a risk-based approach, which would help promote innovation in the technology-side of the financial services sector, while still ensuring the appropriate level of protection. Article 55 should be revised to require risk assessments to be conducted, and records to be retained, only in situations which are likely to result in

[13] Available at: https://fsscc.org/october-25-2018/. (English version only).
可于以下网址查阅：https://fsscc.org/october-25-2018/（仅有英文版）

	Chapter 5 (Articles 51 to 58) on data protection, which should apply to ALL aspects of personal information processing. We submit that complying with Articles 51 to 58 should mitigate the risks of personal information processing in "business as usual" situations.	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 or similarly significantly affecting the individual" and where no method other than ADM is used to produce the result. This is in line with international norms, including the GDPR (Article 35.3(a)).
第五十五条	根据第五十五条，需要对大量的活动进行风险评估。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（第五十一条至第五十八条）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，遵守第五十一条至第五十八条规定，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，这有助于促进金融服务业的技术层面创新，又能确保保护水平处于适当程度。 第五十五条条文应作调整，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"会产生涉及到个人或对个人产生类似的显著影响的法律后果"，而且除了自动化决策系统外没有其他方法的情形下，方会触发风险评估。这与国际规范（包括 GDPR（第35.3(a)条））是一致的。
56	Article 56 requires notification to be made to the relevant authorities and impacted individuals of 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	We recommend clarifying that the scope of a "personal information leak" that must be reported only relates to cybersecurity breaches and should be determined 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. As suggested in our comments on the First Review PIPL, such an approach (which also follows our interpretation of Article 10.1(c)(3) of the 2020 Specification) would also allow

	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.	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. Separately, we suggest expressly providing that a personal information leak or other disclosure within the same organisation or corporate group, including between and among different branches, should not require notification as there should be no risk to data subjects.
第五十六条	第五十六条规定，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	我们建议，应清晰界定必须通知的"个人信息泄露"所涵盖的范围仅涉及网络安全方面的违法，并且应采用风险为导向的评估方法确定；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。如同我们就个人信息保护法（草案一次审议稿）提出的反馈意见，这样的方法（与我们对 2020 年规范第 10.1(c)(3)条的解读）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，

	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。	GDPR 规定的 72 小时时间表是不现实及不切实际的。 另外，我们建议明确规定，在同一机构或公司集团内部（包括在不同分支机构之间）的个人信息泄漏或其他披露不应被要求作出通知，毕竟这种情况下对数据主体不会产生风险。
58	We note that the Second Review PIPL extends obligations of an entrusted party (i.e. data processors in GDPR parlance). In the same way that the GDPR imposes direct regulation on these "data processors", the Second Review PIPL imposes obligations under Chapter 5 of the PIPL on parties that are entrusted with processing personal information on behalf of others.	We assert that this may be a major change for some service providers to financial institutions that have previously not been directly regulated as entrusted data service providers. As such, we would recommend that further guidance is provided by the PRC authorities to ease this transition.
第五十八条	我们注意到个人信息保护法（草案二次审议稿）将义务延伸至涵盖受托方（也就是 GDPR 中的数据处理者）。与 GDPR 对这些"数据处理者"实施直接监管的方式相同，个人信息保护法（草案二次审议稿）在个人信息保护法第五章对接受其他人士委托处理个人信息的受托方规定了相关义务。	我们认为，对于过去作为受托数据服务供应商而没有受到直接监管的金融机构的某些服务提供商而言，这可能是一项重大改变。因此，我们建议中国立法机构提供进一步的指导以帮助顺利过渡。
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**		
59	This article provides that the following constitute the "authorities charged with fulfilling personal information protection duties and responsibilities": (a) the CAC is responsible for comprehensive planning and cooperation and relevant regulatory supervision; (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 government at or above the county level shall fulfil the personal information protection, supervision and management	We make the following recommendations here as for the First Review PIPL: **(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. This is particularly important given the growth in banking services on a national scale, so that reliance on local authorities to supervise multiple entities or branches of the same financial institutions is not feasible without the

	duties and responsibilities determined pursuant to relevant state regulations. The involvement of multiple authorities 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.	potential consistent approaches across the country. We recommend that the lead regulator for financial institutions should be the PBOC, an authority that would know the 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 of the same personal information which may be used in multiple locations. **(c) Details on how different authorities will co-operate 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.
第五十九条	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和相关监督管理工作； (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。	我们就个人信息保护法（草案一次审议稿）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。考虑到全国范围内银行服务的增长，这一点尤其重要，因此，如果无法在全国范围内实行一致性的监管，那么依靠地方监管机构来监督同一金融机构的多个实体或分支机构是不可行的。

	我们担心牵涉多个部门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。 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。
60(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.
第六十条第三款	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。
61	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. In addition, we request that industry stakeholders are regularly consulted on technical and operational issues to ensure that any standards are effective in growing “Digital China” as envisaged under the 14th Five Year Plan.
第六十一条	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。此外，我们还建议就技术和运营

		问题定期与行业利益相关方进行磋商，以确保任何标准均能有效地按照“十四五计划”的设想来建设发展“数字中国”。
62	We submit that 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 processing activities; and • the approval procedures that they need to go through to request information for the purpose of investigations.
第六十二条	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。
63	The ability of the PRC authorities to require the appointment of a professional institution to conduct a compliance audit on personal information processing has been moved to Article 63 of the Second Review PIPL from Article 53 of the First Review PIPL. 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 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.

第六十三条	中国相关部门要求委托专业机构对个人信息处理活动进行合规审计的规定从个人信息保护法（草案一次审议稿）中的第五十三条移至个人信息保护法（草案二次审议稿）中的第六十三条。 不太明确的是：进行合规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（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。
64	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 the manner, timing and scope of enquiries and complaints to be addressed would support an organisation's timely response.
第六十四条	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的方式、时间及范围作出详细界定，将有助于相关机构及时作出回复。
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。
Chapter VII Legal Liability **第七章 法律责任**		
65	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	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. This would enable enterprises to properly understand their risk exposure for

	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.	non-compliance and would also be proportionate to the purpose of the PIPL.
	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。这将使企业能够正确理解其不合规的风险，也将与个人信息法的立法目的相称。
	(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 personal liability involved, it is crucial for senior management of financial services firms to understand the scope of these terms.	We suggest clarifying the definitions of "officer directly in charge" and "other directly responsible personnel". We also recommend that the threshold for 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 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	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

	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。	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	Article 253 of the PRC Criminal Law states that the unlawful provision of personal information to another person may amount to a serious violation of law where between 50 to 5,000 items of personal information are shared. In the modern digital economy, this threshold would be easily surpassed.	We suggest that the relevant authorities consider amending the PRC Criminal Law or arranging further guidance to ensure any violations of criminal law do not lead to unduly onerous sanctions relative to the practical realities of data flows in China's digital economy today.
第七十条	中国刑法第二百五十三条规定，非法向他人提供个人信息在五十条以上五千条以下应当认定为"情节严重"。在当今的数字经济背景下，很容易达到这一判定标准。	我们建议有关机关考虑修订中国刑法，或出台进一步的指引，确保在当今中国数字经济数据流动的实际情况下，不会因违反该条刑法规定的行为招致过于繁重的惩罚。
73	We note that no timetable is stated in the Second Review PIPL 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.
第七十三条	我们注意到，个人信息保护法（草案二次审议稿）没有说明个人信息保护法的生效日期。	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。