Cyberspace Administration of China,

国家互联网信息办公室

No. 11, Che Gong Zhuang Da Jie, Xicheng Qu

北京市西城区车公庄大街 11 号

Beijing Shi, People's Republic of China

北京市，中国

security@cac.gov.cn

24 June 2019

2019 年 6 月 24 日

Dear Sir/Madam

尊敬的先生/女士

RE: The Consultation Draft of the Measures on Data Security

关于：《数据安全管理办法》征求意见稿

The Global Financial Markets Association ("**GFMA**")[1] welcomes the opportunity to submit comments and suggestions on the Measures on Data Security *(《数据安全管理办法》)* (the "**Data Security Measures**") issued by the Cyberspace Administration of China (the "**CAC**").

全球金融市场协会(**"GFMA"**)很荣幸有机会就国家互联网信息办公室（**"贵办公室"**）发布的《数据安全管理办法》提出意见和建议。

GFMA members appreciate the efforts made by the CAC to promote a formal regulation to harmonise the fragmented rules and standards in the area of data security and usage, and provide more specific guidance on the content of data security. We believe that the Data Security Measures will constitute an important part of the fast-developing Chinese data protection legal framework.

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

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

GFMA 成员赞赏贵办公室为促进该项法规正式制定所做的努力，该法规旨在协调数据安全和使用领域的各项规则和标准，并对数据安全的内容提供更具体的指引。我们相信，《数据安全管理办法》必将成为快速发展的中国数据保护法律框架的重要组成部分。

In this letter, we seek clarifications on the application of, and suggest amendments to, certain provisions of these Data Security Measures with the aim to strike a better balance among the data security, privacy protection and the economic usage of data, and provide clearer guidance for network operators to comply with.

在本函中，我们希望能明确《数据安全管理办法》中的部分条款适用问题，并谨对部分条款提出修改建议，旨在更好地平衡数据安全、隐私保护和数据的合理使用，并为网络运营者提供更清晰的行为准则。

1. Important Data

1. 重要数据

Article 28 requires network operators to complete security assessment and obtain consent from the sectorial regulators before providing important data offshore.

第 28 条要求网络运营者在向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意。

Firstly, "Important data" is defined in Article 38 (5), but the current definition is broad and does not provide a practical evaluation criteria, without which, network operators will experience difficulties in identifying the important data that they may possess. As each industry has different characteristics and sectorial considerations, we sincerely hope that sectorial regulators/supervisors will be involved in formulating evaluation criteria of important data with respect to their particular industry, as was contemplated by the 2017 "Personal Information and Important Data Cross-Border Security Assessment Measures".

首先，虽然第 38 条第 5 款规定了"重要数据"的定义，但该定义较为宽泛，且缺乏有操作性的评价标准；因此，网络运营者在识别他们可能拥有的重要数据时可能会遇到困难。鉴于每个行业特性不同，考量因素也相应不同，我们真诚地希望行业主管监管部门能够参与制定基于特定行业的重要数据评估标准，正如 2017 年《个人信息和重要数据出境安全评估办法》中所规定的。

Secondly, the Cybersecurity Law of the People's Republic of China only requires operators of critical information infrastructure ("**CIIO**") to conduct security assessment before transferring important data offshore, however, Article 28 appears to expand the scope of the security assessment requirement to cover all network operators. Article 28 further creates a new requirement for network operators to obtain regulators' consent before transferring important data offshore. Whilst we appreciate CAC's efforts in safeguarding the internet environment, we believe cross-border information transfer should be permitted in principle, and the regulators' consent only sought in exceptional and limited circumstances. Given the broad definition of "network operator", it appears that almost all companies operating online businesses will fall into the scope of Article 28. This requirement will be particularly problematic to the onshore presences of international financial institutions whose home regulator may request information for integrated risk control purposes or which require information to be transmitted to senior management located outside the country. International financial institutions do not want to be put at risk of non-compliance with their home regulators' requests for information which take place in jurisdictions other than the People's Republic of China. We sincerely hope that the Data Security Measures can align with the Cybersecurity Law that limit the application scope of Article 28 to only CIIOs. At least, the regulators' consent shall only be required in limited cases and exemptions shall be provided for data to be transferred

for purposes including group risk management and performance of mandatory requirements (such as know-your-client or anti-money laundering).

其次，《中华人民共和国网络安全法》仅要求关键信息基础设施运营者(**“CIIO”**)在向境外传输重要数据前进行安全评估，但第 28 条似乎将安全评估要求的范围扩大至所有网络运营者。此外，第 28 条还提出了一项新要求，网络运营者在向境外传输重要数据前，必须获得监管部门的同意。我们赞赏国家互联网信息办公室为维护互联网环境所做的努力，但我们同时认为，原则上应当允许信息的跨境传输，只有在特殊和有限的情况下，才需要征求监管部门的同意。“网络运营者”的定义较为宽泛，似乎几乎所有在线经营业务的公司都将落入第 28 条的适用范围。而这一要求尤其对国际金融机构的境内实体造成了困扰，这些机构的母国监管机构可能为综合风险控制的目的要求提供信息，或要求将信息传递给位于国外的高级管理人员；国际金融机构不希望面临违反母国监管机构提供信息要求的合规风险，而这都将在中国以外的法域发生。因此，我们真诚地希望《数据安全管理办法》能够与《网络安全法》的规定相一致，将第 28 条的适用范围限制为关键信息基础设施运营者。至少，只有在有限的情况下才需要获得监管部门的同意；同时，应当为基于集团风险管理和执行强制性要求等目的的数据传输（如“了解你的客户”或反洗钱）提供豁免条款。

Thirdly, there is an absence of detailed regulatory guidance on how network operators should conduct security assessments. Obtaining regulators' consent prior to each posting, sharing, trading and providing important data offshore would incur administrative burden and substantial uncertainty for international companies, which may use their offshore data centre to supervise onshore activities for internal compliance purposes. Without further detailed guidance, it would be difficult for them to comply with this article when conducting cross-border business or conducting onshore business with international financial groups. Therefore, we seek clarity regarding the content and the procedure of security assessments, and the procedures to obtain regulators' consent.

第三，《数据安全管理办法》缺乏关于网络运营者如何进行安全评估的详细监管指导。每次在境外发布、分享、交易和提供重要数据之前，都要获得监管部门的同意，这将给跨国公司带来行政负担和巨大的不确定性，因为他们一般会利用境外数据中心来监控境内活动，以实现内部合规目的。如果没有进一步的详细指导，网络运营者在开展跨境业务或与国际金融集团开展境内业务时，将难以遵守本条规定。因此，我们希望明确安全评估的内容和程序，以及获得监管部门同意的程序。

2. Exemptions for Security Assessments

2. 安全评估的豁免

Article 27 requires a network operator to complete a security assessment and obtain consent from a data subject before providing personal information to any other party, with limited exemptions. These exemptions are not the same as those described under the Information Security Technology - Personal Information Security Specification ("**Specification**"), which came into effect in May 2018 (e.g. "safeguarding the major lawful rights and interests such as life and property of PI subjects and other individuals, and it is difficult to obtain consent from personal information subject", "performing the legal obligations of the data controller", "where the information is obtained from public domain", which are exemptions under the Specification and are not included in the Data Security Measures). Whilst the Specification is a national standard without mandatory effects, it serves as an important guidance to all market participants and a part of the privacy protection legislation framework. We therefore suggest that the exemptions under these two rules should be aligned.

第 27 条规定网络经营者在向他人提供个人信息前，应当评估可能带来的安全风险，并征得个人信息主体同意，但允许个别的例外情形。这些例外与 2018 年 5 月生效的《信息安全技术——个人信息安全规范》(以下简称**“《规范》”**)所规定

的例外并不相同。（例如，《规范》规定的例外包括出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的、为履行信息控制者法定义务所必需的、信息从合法公开披露的信息中所获得的；但这些例外并未被包含在《数据安全管理办法》内。）虽然《规范》不是一个强制性国家标准，但它对所有市场参与者来说仍是一个重要的指引，同时也是隐私保护立法框架的重要组成部分。因此，我们建议这两项规则下的例外情形应保持一致。

In addition, it is increasingly being recognised in the European Union that it is difficult to pre-conceive every complete operational/administrative use of data. For example, in the corporate context, it is important for a company to be able to conduct due diligence on a potential target which can involve some personal data (even if substantial amounts are redacted), but seeking consent from every data subject is not practical and would jeopardize confidentiality requirements. Considering these practical difficulties, we suggest incorporating in Article 27, the exemptions set out in the Specification as well as the following additional exemptions:

此外，欧盟愈发认识到，很难预先设想好数据的每一个完整的业务或行政用途。例如，在公司中，对一个潜在的目标进行尽职调查是十分重要的，其中就可能涉及到一些个人数据（即使大部分已经编辑处理），在此种情况下，寻求其中涉及到的每一个个人信息主体的同意是不现实的，并会违反保密要求。考虑到这些实际困难，我们建议在第 27 条中加入《规范》中规定的豁免情形，并额外增加以下例外情形：

(i) To discharge the know-your-client or anti-money laundering or other legal or regulatory obligations; and

为履行“了解你的客户”、反洗钱或其他法律或监管义务；及

(ii) If there are legitimate grounds and it is reasonable and necessary to process such personal data without consent.

有合法理由，且未经同意处理该等个人信息是合理且必要的。

3. Obligations in Relation to Third Parties

3. 第三方责任

Article 14 stipulates that direct collection and indirect collection of personal information shall subject the network operator to “equal”/ “the same” protection responsibility and obligation. We appreciate that it may be reasonable to require the same level of protection in terms of data storage and usage, however, in the case where the network operator obtains personal information through third parties, the network operator does not have a direct relationship with the data subject, the network operator will not be able to obtain the data subject’s consent nor be able to notify the data subject directly. We respectfully request that the CAC further clarify the meaning of, and to what extent the obligation or responsibilities should be “equal”/ “the same”.

第 14 条规定，网络运营者从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。我们认可，对数据的存储和使用进行同等级别的保护可能具有合理性；但是，在网络运营者通过第三方获得个人信息的情况下，网络运营者和个人信息主体没有直接的关联。网络运营者无法获得个人信息主体的同意，也无法直接通知个人信息主体。我们谨要求国家互联网信息办公室进一步明确“同等”/“相同”的含义，以及在何种程度上义务或责任应该是“同等的”/“相同的”。

Article 30 imposes on network operators the obligation to monitor third-party applications connected to its platform, and the responsibility to indemnify the users’ loss on presumption of fault. We would like to note the observations and suggestions in relation to this provision:

第 30 条规定网络运营者有义务督促接入其平台的第三方应用者加强数据管理，并根据过错推定原则向用户承担第三方应用造成损失的赔偿责任。我们愿就这一规定提出意见和建议：

(i) The concept and scope of third-party applications are relatively new in legislations and there is no clear definition, hence we hope that the CAC may provide more clarity in this respect;

第三方应用的概念和范围在立法上相对较新，也没有明确的定义，因此我们希望贵办公室能在这方面提供更清晰的定义；

(ii) The reasons for providing data to third parties vary. Sometimes the data is provided due to the network operator's business needs, and sometimes the data provision is requested from or instructed by the users to fulfil the user's specific needs. We strongly recommend that the CAC differentiate the obligation and responsibility imposed on network operators according to their relationship with third parties. In particular, the network operator should not be held liable if the provision or sharing of data is initiated or requested by the user; and

向第三方提供数据的理由各不相同。有时是由于网络运营者的业务需要，有时是为了满足用户的特定需求。我们强烈建议贵办公室根据网络运营者与第三方的关系来区分网络运营者的义务和责任。特别是，在用户发起或要求提供或共享数据的情况下，网络运营者不应承担责任；及

(iii) The principle of presumption of fault imposed on the network operator to prove otherwise is extremely high and not practical. We seek clarification on the minimum proof for network operator of being "no fault". In this regard, network operators should not be held liable if they have taken reasonably practicable steps to ensure data security.

过错推定原则对网络运营者施加了过高的证明要求，同时也不具有可操作性。我们请求厘清对网络运营者"无过错"的最低证明要求；即网络运营者如已采取合理可行的措施保证数据安全，则无须承担责任。

4. Regulatory Reporting/Client Notification

4. 监管报告/客户通知

Article 15 states that if network operators collect important data or sensitive personal information for business purposes, network operators shall file with the local CAC. Given the broad definition of "important data", "sensitive personal information" and "business purposes", most data collection activities would fall foul of filing requirements, and such administrative burdens to network operators and regulators do not offer obvious benefits in risk management. As network operators are likely to already be subject to laws and regulations which require accountability, network operators should be permitted to maintain their own files in relation to their collection and use of important data or sensitive personal information for business purposes. In other words, we respectfully suggest removing the filing requirement; at most, network operators can be required to report on a case-by-case basis to the CAC. This is consistent with the approach adopted for GDPR[2]. Alternatively, we suggest restricting the filing requirements only to CIIOs.

[2] Under the European Union 1995 Data Protection Directive, organizations are required to notify or register certain personal information processing activities with the regulators. This caused unnecessary and extensive administrative burdens on both regulators and businesses. As a result, the European Commission proposed its comprehensive reform and replaced the Directive with GDPR, removing many of the filing requirements which helped businesses to save approximately billions of Euro per year, including paperwork costs.

第 15 条规定，网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。鉴于“重要数据”、“个人敏感信息”、“以经营为目的”的定义都很宽泛，绝大多数数据收集行为都将触发备案要求。这对网络运营者及监管部门造成了行政负担，但对风险管理来说并无明显益处。由于网络运营者很可能已经受到法律和法规的约束，网络运营者本就需要根据该等法律和法规承担责任，因此应当允许网络运营者保留自己以经营为目的收集和使用重要数据或个人敏感信息的文件。换言之，我们真诚地建议取消备案要求，网络运营者最多需要根据要求向网信部门报告个案；这与 GDPR 所采用的方法是一致的。或者，我们建议仅对关键信息基础设施运营者适用备案要求。

Also, we appreciate clarity as to what constitutes “collection for business purpose”. Many network operators may collect important data or sensitive personal information in the course of their business activities but not collecting data as their core business functions. Without specifying the threshold (e.g. volume or high-risk level where huge quantities of individuals are involved), the existing obligation contemplated under the draft rule is extensive.

此外，我们希望对“以经营为目的的收集”的定义进行厘清。许多网络运营者在其经营活动中可能会收集重要数据或个人敏感信息，但不将收集数据作为其核心业务功能。征求意见稿并未明确该等判断标准（例如涉及大量个人信息或高风险水平），因此会导致其所规定的义务过于宽泛。

Article 35 requires that in the event of personal information leakage, damage, loss and other data security incidents, or where the likelihood of data security incidents taking place is significantly increased, network operators shall immediately take remedial measures to inform the data subjects and regulators. In practice, minor data security incidents may not incur material harm to data subjects, we respectfully suggest that such notification requirement should only apply to incidents that may cause serious risk of harm but not to any data incident. Also the time frame is much more stringent relative to that of GDPR and other equivalent laws and regulations in other foreign jurisdictions. We would recommend a more practicable timeframe, e.g. “without undue delay upon becoming aware.”

第 35 条规定，发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，网络运营者应当立即采取补救措施，告知个人信息主体和监管部门。实践中，轻微的数据安全事件可能不会对个人信息主体造成实质损害，我们建议该等通知要求仅适用于可能极易导致损害风险的事件，而不是适用于所有数据安全事件。此外，与 GDPR 及其他法域的相关法律法规相比，《数据安全管理办法》在时间上的要求过于严苛。我们建议设置一个更切实可行的时间要求，例如“在获知不得无故拖延”。

Article 36 stipulates that authorities may require network operators to provide data under certain circumstances. While such requirements may be necessary, we suggest more details are provided with respect to the particular circumstances and safeguards being put in place, ensure that the data required by the relevant competent authorities are directly relevant and necessary to perform their respective responsibilities, a legitimate and centralised channel should be established to provide these data, and given the practical difficulty for regular employees to verify the identification of the officers, joint collaboration by and supervision of sectorial regulators would be preferable.

第 36 条规定，有关主管部门在某些情况下可能会要求网络运营者提供数据。尽管主管部门的要求可能是必要的，但我们依然建议明确适用的具体情形，做好保障措施，以确保有关主管部门获取数据与其履行职责是直接相关且必要的。同时，

根据欧盟 1995 年的《数据保护指令》，各组织必须向监管机构通报或登记某些个人信息处理活动。这给监管机构和企业带来了不必要的、广泛的行政负担。因此，欧盟委员会提出了全面改革方案并用 GDPR 取代了《指令》，这使得许多备案要求被取消，每年帮助欧洲节省了约数十亿欧元，包括日常文书成本。

应当建立一个合法且集中的渠道来统一提供这些数据。实践中，普通雇员难以真正核实主管部门人员的身份，因此最好由行业主管监管部门牵头进行合作和监督。

5. Other Clarifications

5. 其他需要明晰的部分

(i) Article 8 stipulates that the rules of collection shall indicate the name of the person in charge of data security, which seems to suggest all network operators must have a person in charge of data security. However, Article 17 suggests that only network operators who collect important data or sensitive personal information must specify the person in charge of data security. We appreciate clarity be provided in this regard and suggest "if applicable" being added to Article 8 to limit the application of the term "person in charge of data security."

第 8 条规定了收集规则应当指出数据安全责任人的姓名，这似乎要求所有的网络运营者必须设置数据安全责任人。但是，根据第 17 条的规定，只有收集重要数据或个人敏感信息的网络运营者应当明确数据安全责任人。我们希望这一方面能够得以明确，同时建议在第 8 条增加“如适用”以明确“数据安全责任人”的有限适用性。

(ii) Article 23 regulates "direct push", which seems to refer to Cookies and Marketing Opt-Out practices, but we respectfully suggest clarification be provided in this regard. In addition, when conducting direct push, network operators must honour "social moralities" and "business ethics", and such terms appears to be vague and we suggest be defined more narrowly.

第 23 条规定了“定向推送”内容，似乎指的是信息记录程序和推广退订实践，但我们建议这点能够得以明确。此外，在进行定向推送时，网络运营者应当尊重社会公德、商业道德；这些用语的外延较为模糊的，我们建议进行更明确且狭义的定义。

(iii) Article 29 requires that where a domestic user accesses a domestic network, the traffic shall not be routed offshore. We sincerely request CAC provide clear definitions for "domestic user" and "domestic network." Any implications of internet not being able to be routed outside the country is unrealistic and impractical.

第 29 条规定，境内用户访问境内互联网的，其流量不得被路由到境外。我们真诚地希望贵办公室对“境内用户”、“境内互联网”进行更清晰的定义。在实践中，不得将互联网的流量导出境外并不现实或具有可操作性。

GFMA greatly appreciates the CAC's consideration of the points and questions raised in this letter and would be pleased to discuss them in greater detail. If you have any questions, please contact Erik Bainbridge, Manager Policy and Regulatory Affairs at ebainbridge@asifma.org or Tel: +852 2531 6562. This submission was prepared by PRC law firm Fangda Partners, GFMA, and its affiliates' members.

GFMA 非常感谢贵办公室考虑本函提出的观点和问题，并很乐意更详细地讨论这些问题。如果您有任何疑问，请联系政策和法规事务经理埃里克·班布里奇先生（电邮 ebainbridge@asifma.org 或电话+85225316562）。本函由上海市方达律师事务所、GFMA 以及其会员共同撰写。

Yours sincerely,
顺颂商祺，

Kenneth E. Bentsen, Jr.
CEO, Global Financial Markets Association and
President and CEO, Securities Industry and Financial Markets Association
全球金融市场协会首席执行官 及
证券业和金融市场协会首席执行官兼主席