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

12 July 2019

2019 年 7 月 12 日

Dear Sir/Madam:
尊敬的先生/女士:

RE: The Consultation Draft of the Measures for Security Assessment of Personal Information Outbound Transfer

关于：《个人信息出境安全评估办法》征求意见稿

The Global Financial Markets Association ("**GFMA**")[1] welcomes the opportunity provided by the Cyberspace Administration of China (the "**CAC**") to submit comments and suggestions on the draft Measures for Security Assessment of Personal Information Outbound Transfer (《个人信息出境安全评估办法》) (the "**Outbound Transfer Measures**")[2].

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《个人信息出境安全评估办法》（《评估办法》）提出意见和建议。

---

[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

[2] http://www.cac.gov.cn/2019-06/13/c_1124613618.htm

GFMA appreciates the CAC's efforts to further develop the current rules and standards relating to cross-border transfers of personal data. We also note and support the commitment of the Chinese government at the recent G20 summit in Osaka to harness the full potential of data and the digital economy and maximise the benefits of digitisation[3].

GFMA 十分赞赏贵办公室为了进一步发展与个人数据跨境传输相关的现有规则和标准所作出的努力。我们注意到中国政府最近在大阪举办的 G20 峰会上，亦作出了充分挖掘数据和数字经济的潜力并致力于最大化数字时代效用的承诺，我们对此表示支持。

In this letter, we seek clarification on the application of, and suggest amendments to, certain provisions of the draft Outbound Transfer Measures with the aim of striking a better balance between data security, privacy protection and the economic usage of data (including information sharing), and to achieve clearer compliance guidance for Network Operators.

在本函中，我们希望能明确《评估办法》（征求意见稿）中的部分条款的适用问题，并谨对部分条款提出修改建议，旨在更好地平衡数据安全、隐私保护和数据的经济利用（包括信息共享），并为网络运营者提供更清晰的合规指导。

1. Application to Regulated Financial Institutions
对受监管的金融机构的适用

Regulated financial institutions are already subject to information security and data protection requirements and are already regulated by sectoral regulators such as PBOC and CBIRC. This puts them in a very different position to unregulated corporate entities which may have no data protection processes in place. PBOC already has rules in place in respect of personal data protection for bank clients[4].

受监管的金融机构本身已经受到信息安全和数据保护要求的约束，包括中国人民银行和中国银行保险监督管理委员会等行业监管机构提出的要求。这使得它们与其他未受监管的公司实体完全不同，这些公司实体可能目前并不具备数据保护机制。而中国人民银行就银行客户的个人数据保护已经制定了相关规定。

It is unclear how the Outbound Transfer Measures will interact with local banking regulators' rules on this topic and how financial institutions are meant to comply with potentially inconsistent

[3] https://www.meti.go.jp/press/2019/06/20190628001/20190628001_01.pdf

[4] Notice of the People's Bank of China for Banking Financial Institutions to Get the Personal Financial Information Protection Work Well Done (effective from 1 May 2011, available here)
《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（2011 年 5 月 1 日生效，全文请参见此处）

requirements at the same time. For instance, where a personal data subject requires that data be deleted, this may conflict with a regulatory record keeping requirement.

目前我们尚不清楚《评估办法》与各地银行业监管部门的相关规定之间会产生何种影响；亦未明确金融机构在该等规定产生矛盾之时，应当如何遵守。例如，当个人信息主体要求删除数据时，这可能会与金融监管所要求的保存记录相冲突。

To maintain consistency and encourage efficiency we sincerely suggest allowing PBOC/CBIRC to act as the relevant authority in respect of data protection matters for regulated financial institutions instead of CAC. This would enable CAC to focus on unregulated corporate entities, technology and social media companies.

为了保持一致性并提高监管效率，我们诚挚地建议由中国人民银行/中国银行保险监督管理委员会担任受监管金融机构的数据保护监管机构，而非网信部门。这样，网信部门能够有更多精力专注于未受监管的公司实体、技术和社交媒体公司。

2. Cross Border Data Transfer Mechanisms and CAC Security Assessments
跨境数据传输机制与网信部门安全评估

From a practical point of view, we sincerely suggest CAC considering:

从操作层面考虑，我们诚挚地希望贵办公室考虑如下建议：

1) Permitting Network Operators to conduct their own security assessment according to the standards provided under Article 6, as well as relying on Template Contracts (see below) instead of submitting materials to CAC under Article 4 of the draft Outbound Transfer Measures. Such information would still be available on request to the CAC pursuant to Articles 8 and 10. This approach would be aligned with the one taken in the previous released draft of Measures for the Security Assessment of Personal Information and Important Data Outbound Transfer（《个人信息和重要数据出境安全评估办法》）which provide that the assessment may be conducted by Network Operators themselves, industry regulators or network regulators according to different thresholds[5].

[5] The draft is released on 11 April, 2017, available here.
The relevant articles are cited as below:
Article 7 Prior to transmitting data abroad, a network operator shall organize on its own the security assessment for the data to be transmitted abroad, and be liable for the assessment results.
Article 9 In any of the following circumstances, a network operator shall apply to its industrial authority or regulator to organize security assessment: (1) The data to be transmitted abroad contains or contains in aggregate the personal information of more than 500,000 users; (2) The quantity of the data to be transmitted abroad is more than 1,000 gigabytes; (3) The data to be transmitted abroad contains data in the areas of nuclear facilities, chemical biology, defense industry, population and health, as well as the data of large-scale project activities, marine environment and sensitive geographic information; … (6) Other data which may affect national security, and social and public interests, and are necessary for assessment as determined by the industrial authority or regulator.

相较于根据《评估办法》第四条向网信部门提交大量材料，应当允许网络运营者根据《评估办法》第六条所规定的标准自行进行安全评估，并且依靠模板合同（见下文详述）达到要求。当然，根据《评估办法》第八条和第十条，在网信部门提出要求时，此类信息仍将被提供。这样的方式与贵办公室此前发布的《个人信息和重要数据出境安全评估办法》（征求意见稿）保持一致；该征求意见稿规定：网络运营者可以自行进行安全评估，在到达一定门槛时，由行业监管部门或网信部门进行安全评估。

2) Only requiring a CAC security assessment for operators of critical information infrastructure.
仅对关键信息基础设施运营者适用安全评估的要求。

3) Clarifying that where the CAC has not responded to any security assessment provided to it within the 15-day timeframe, that business may proceed with the relevant data transfer on the assumption that the CAC has no objections. This does not preclude the CAC from raising objections at a later date for future transfers.
明确如果网信部门未在 15 天的时限内就申报的安全评估作出回复，经营主体可以默认网信部门无异议而进行相关的数据传输。当然这并不妨碍网信部门在此后对尚未发生的传输提出异议。

4) Exploration of alternative methods of outbound transfers of personal data, such as binding corporate rules, approved code of conduct or approved certification mechanisms. This would be particularly relevant for intra-group data transfers between entities subject to data protection requirements globally, since multi-national groups apply high and uniform standards of data protection given that they are subject to global rules. It will greatly ease the multinational corporations if regulators could look into such group rules, confirm its

---

If there is no definite industrial authority or regulator, the Cyberspace Administration of China shall organize the assessment.

该征求意见稿发布于 2017 年 4 月 11 日，全文请见此处。

相关条款引用如下：

第七条 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。

第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：

（一）含有或累计含有 50 万人以上的个人信息；（二）数据量超过 1000GB；（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；……（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

行业主管或监管部门不明确的，由国家网信部门组织评估。

effectiveness on data protection, then do not conduct security assessment over intra-group data transfer anymore.

探索个人数据出境传输机制的替代方式，例如公司内部约束机制、经批准的行为准则或经批准的认证机制。这一点对于集团内实体间的数据传输来说尤为重要；它们需要在全球范围内满足数据保护要求，因此，跨国集团在数据保护方面，往往适用非常高的统一标准。如果监管部门能够审查跨国集团的该等政策，并相应认可其在数据保护上的有效性且不再对集团内的数据传输进行安全评估，这将提供极大的便利。

5) Adopting a "white list" approach whereby transfer to a recipient which is in a specific jurisdiction, corporate group, or which is supervised by a regulatory authority does not require a security assessment. A "white list" approach will increase commercial efficiencies by permitting cross-border transfers conducted by pre-approved companies and will align to international practice.

采用"白名单"机制：即当信息接收者位于特定的司法管辖区、集团或受到其他部门监管时，向这些接收者进行数据传输时，不需要进行安全评估。"白名单"机制将允许预先经过批准的公司直接进行跨境传输，这能够提高商业效率，亦与国际实践保持一致。

Internationally, laws, regulations and regulatory practices relating to data protection are recognising the need to remove administrative burdens and obstacles to the free flow of data into and out of jurisdictions and replacing these with enhanced data governance obligations with clearer accountability. In this context, regulatory approval of cross border transfers has always been very limited, and under the 2016 European rules, does not exist in most instances.

在国际上，与数据保护相关的法律、法规和监管实践均意识到需要消除限制不同法域数据自由流动的行政负担，并逐渐将这些限制转换成具有明确问责机制的加强型数据治理义务。在这种环境下，需要进行监管审批的跨境传输十分有限；根据 2016 年欧盟相关规则，甚至大部分情形下都不存在此种监管批准。

The European Union's 2016 General Data Protection Regulation[6] (the **"GDPR"**) has created multiple methods for transferring personal data out of the EU to other jurisdictions. The most popular method is the use of template contractual clauses between the EU entity providing the data and the non-EU recipient (a **"Template Contract"**). No regulatory approval is needed to transfer personal data outside

[6] The GDPR is available here, and Article 46 (2) sets out cross border transfer processes that do not require any specific authorisation from a supervisory authority.

GDPR 请参见此处，第 46（2）条规定了不需要获得监管授权的跨境传输流程。

the EU if using a Template Contract. This has simplified and greatly reduced administrative burdens on businesses. The form of Template Contracts were agreed in partnership with the private sector and are published online[7].

欧盟 2016 年通用数据保护条例（"GDPR"）创造了从欧盟向其他法域传输个人信息的多种方法。被采用最多的方法是在欧盟的转出方和非欧盟的接收者之间使用模板合同条款（"模板合同"）。在使用模板合同时，将个人信息传输至欧盟之外的地方无需经过监管批准。这简化了行政程序并大大减少了经营者的行政负担。模板合同的内容是与行业共同制定的，并在网上公布。

The Template Contracts are not the only method of transferring personal data out of the EU. Article 46 of the GDPR provides various other methods of doing so, for example binding corporate rules, approved code of conduct or an approved certification mechanism. We would be happy to provide further information on these methods to the CAC.

模板合同并不是向欧盟外传输个人信息的唯一方式。GDPR 第四十六条亦规定了各种各样方式均可达到同样效果，例如公司内部约束机制、经批准的行为准则或经批准的认证机制。我们很乐意为贵办公室进一步提供关于这些方式的更多信息。

From this perspective, the requirement for a CAC security assessment in all circumstances pursuant to Article 5 of the draft Outbound Transfer Measures is not in alignment with international standards and will create significant (and unnecessary) administrative burdens and costs for businesses.

从这个角度来看，《评估办法》第五条所规定的在所有情况下均由省级网信部门进行安全评估并不符合国际标准，并将给经营者带来巨大的（且不必要的）行政负担和经营成本。

In addition, given (i) the sizeable number of businesses that would need to apply to CAC to a conduct security assessment, (ii) the fact that assessments are required on a per-recipient basis, (iii) the fact that assessments must be renewed upon changes to the purpose, type or overseas storage period of the transfer (and in any case every two years), and (iv) the commitment for CAC to complete security assessments within 15 days, Article 5 of the draft Outbound Transfer Measures may be an impractical burden for CAC itself in terms of time and resources, and will cause significant disruption to day to day businesses if delays in CAC assessments occur.

此外，鉴于(i)大量经营者需要向网信部门申请进行安全评估，(ii)向不同的接收者提供个人信息应当分别申报安全评估，(iii)个人信息出境目的、类型和境外保存时间发生变化时（以及不论何种情况下每两年）必须重新评估，及(iv)网信部门承诺在 15 天内完成安全评

[7] The Template Contracts are available here. In particular, CAC may wish to look at the contract set out in the Annex here.
模板合同规定请参见此处。特别地，贵办公室可以参见附件中列明的合同。

估，《评估办法》第五条可能对于网信部门本身而言是一项在时间和资源方面均不具有操作性的负担。并且，如果网信部门未能按时评估，将会对经营者的日常业务造成重大干扰。

3. Exclusions for Ancillary Business Functions
部分商业行为的豁免

Separate to our points above on methods of transferring personal data on a cross border basis, CAC could consider narrowing the scope of data which is subject to the draft Outbound Transfer Measures.
除上述关于跨境个人数据传输方式的讨论之外，贵办公室亦可考虑缩小《评估办法》适用的信息/数据范围。

Specifically, Article 21, which has provided the definitions, could clarify that personal information that has been redacted/masked is no longer considered as personal information – this would align the draft Outbound Transfer Measures with Article 42 of the Cyber Security Law of People's Republic of China (《网络安全法》) (the "**Cyber Security Law**")[8].
具体而言，《评估办法》第 21 条规定的定义中可以明确已经编辑或模糊处理的个人信息不再属于个人信息的保护范畴——这也与《中华人民共和国网络安全法》（"《网络安全法》"）第四十二条的规定保持一致。

Article 2 could also clarify that the following are not in scope of the draft Outbound Transfer Measures:
《评估办法》第二条亦可以进一步明确在适用范围中排除以下情形：

1) Cross-border payments where personal information is related to a customer instruction such as beneficiary name, account details, contact, etc. (or CAC could otherwise confirm that a customer instruction by its nature implies consent in such instances). Without this clarification a Chinese consumer may not be able to shop online without waiting a minimum of 15 days for CAC approval.

---

[8] Article 42 No network operator may disclose, tamper with or destroy personal information that it has collected, or disclose such information to others without prior consent of the person whose personal information has been collected, unless such information has been processed to prevent specific person from being identified and such information from being restored.
第四十二条网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。
网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

跨境支付中因客户指令而对外传输的个人信息，例如受益人姓名、账户详情、联系方式等等。（或者网信部门可以另行认可，这些客户指令本质上就意味着同意。）若没有这样的豁免，中国客户在线购物需要等待至少 15 天以获得网信部门的批准。

2) Outbound transfers of staff information, internal management or operations managed by headquarters at global/regional level. Many corporate groups have hundreds of subsidiaries and facilitating transfers of information at an intragroup level will greatly ease ongoing administrative burdens. Without this clarification, administrative functions such as hiring decisions or payment of salaries may be impeded.

通过全球或区域总部及性能管理的集团公司的员工信息、内部管理或经营信息的境外传输。许多公司集团拥有成百上千的子公司，简化集团内的信息传输将极大地减轻其承担的行政义务。若没有这样的豁免，集团公司在做出雇佣决定或工资支付这样的行政职能时，可能会有障碍。

3) Data transfers for law enforcement purposes. Without this clarification court proceedings, bankruptcy processes, investigations, handling of complaints and similar matters may be impeded.

以执法为目的的数据传输。若没有这样的豁免，法庭程序、破产程序、调查、投诉处理和类似事项都可能遭遇障碍。

4) Data already transferred abroad (i.e. no retroactive effect or repetitive assessment).

已经传输到境外的数据（即安全评估不存在溯及力且不应重复评估）。

5) Personal information that was collected overseas.

在海外收集的个人信息。

4. Definition of Network Operator and Personal Sensitive Information
网络运营者和个人敏感信息的定义

The Outward Transfer Measures adopt the same definition of "Network Operator" as the one set out in the Cyber Security Law. While this contributes to consistency, the original definition of Network Operator remains broad and unclear. Under this definition, any business or person possessing two computers that can be linked through the internet could be a Network Operator and would be subjected to significant compliance costs pursuant to the relevant regulations. We therefore suggest that the CAC further explain and clarify the scope of Network Operator and revise this definition accordingly (e.g. narrow down the definition to businesses that operate mainly through online platforms) for purposes of the Cyber Security Law more generally (e.g. through public guidance of FAQs).

《评估办法》中采用了与《网络安全法》中的"网络运营者"相同的定义。这样做有助于保持法律法规的一致性，然而，原有的网络运营者的定义本身仍是宽泛且不清晰的。根据该定义，任何拥有两台可以通过互联网链接的电脑的经营者或个人可能成为网络运营者，并根据法律法规将承担巨大的合规成本。因此我们诚恳地建议贵办公室进一步解释并阐明网络运营者的范围，并且为《网络安全法》（例如，通过对常见问题提供公开回答）相应地修改该定义（例如，将该定义限缩至主要通过在线平台运营的经营者）。

The definition of "Personal Sensitive Information", i.e. Personal Information that, once leaked, stolen, tampered, or illegally used, may endanger personal and property safety of the information subject, or cause damage to the reputation and physical and/or mental health of the information subject, can be subjective and vague. It has a different meaning from the meaning generally accepted in jurisdictions other than China, such as the European Union. From the perspective of promoting uniform standards of data protection and efficient cross-border data transfer, we recommend a definition of Personal Sensitive Information that is further aligned to the European Union definition, by including reference to personal data consisting of racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation that is more aligned with international regulatory practices.[9]

当前对"个人敏感信息"的定义，即一旦被泄露、窃取、篡改、非法使用可能危害个人信息主体人身、财产安全，或导致个人信息主体名誉、身心健康受到损害等的个人信息，是主观的且模糊的。它与在中国之外的其他法域例如欧盟所普遍接受的含义存在差异。为了促进数据保护的统一规则和有效率的跨境数据传输，我们建议对于个人敏感信息采用与欧盟定义更加相似的定义，例如包含有种族或民族、宗教或哲学信仰、基因数据、生物识别数据、与健康有关的数据或与自然人的性生活或性取向相关的数据组成的个人数据，这与国际监管实践更相符。

5. Use of Template Contracts
模板合同的使用

[9] The categories of sensitive data are set out in Article 9 of the GDPR, which are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Recital 75 of GDPR sets out the broader context of the legislative intention behind the GDPR. The Recitals are available here.

个人敏感信息的分类请参见 GDPR 第九条，即：能够反映种族或民族、宗教或哲学信仰、基因数据、生物识别数据、与健康有关的数据或与自然人的性生活或性取向相关的个人信息。与 GDPR 相关的立法文件第 75 条揭示了 GDPR 更为广泛的立法目的，请参见此处。

As set out above, the EU GDPR provides that third country transfers are permitted where Template Contracts are used. The draft Outbound Transfer Measures also set out a requirement for a contract between the data exporter and the data recipient. We sincerely seek clarification on whether CAC will work with the private sector to produce a Chinese template contract that can be used more widely. We also seek clarification on whether CAC will permit entities to use the EU's Template Contracts as valid contract templates. Allowing the use of EU Template Contracts will greatly ease the regulatory burden for international businesses which must already comply with GDPR and members' view is that the Template Contracts should generally meet the requirements set out in the draft Outbound Transfer Measures relating to the contract (see also our comments in section 8 below on the draft contractual rights and obligations).

如上所述，根据GDPR规定，当使用了模板合同时，信息的对外传输是被允许的。《评估办法》亦对数据转出方和接收者之间签订的合同提出了要求。因此，我们真诚地希望贵办公室明确网信部门是否会与行业合作出台中国版模板合同，以便跟为广泛的适用。欧盟允许使用模板合同已极大地减轻了对于已经负有遵守GDPR义务的国际经营者的监管负担，并且 GFMA 的成员认为，模板合同能够大体符合《评估办法》中对于合同的要求（亦可参见我们在下文第8部分对于合同权利义务的意见）。

International practice does not mandate specific information security provisions. Instead, the recipient either agrees to abide by a set of general data protection principles (if the recipient will be processing the data for their own, independent purposes), or the sender and recipient agree in their contract on a set of "reasonable and appropriate" security measures (if the recipient will be processing the data solely on behalf of the sender).

国际实践中，监管并不会强制要求适用特定的信息安全规范。相反地，信息接收者可以同意遵守一系列通用数据保护原则（如果接收者将为了其独立目的处理数据），接收者亦可以与转出方在合同中约定一系列"合理且合适的"安全保障措施（如果接收者仅将代表转出方处理数据）。

6. Security Assessments
安全评估

Separate to our earlier comments which seek to reduce the administrative burden on Network Operators and the CAC, in the event that the CAC still needs to perform a security assessment (e.g. for critical information infrastructure), we set out additional recommendations.

除了我们在上文提出的减轻网络运营者和网信部门行政负担的建议之外，如果网信部门仍然需要进行安全评估（如对关键信息基础设施），我们在此另行提出如下建议。

a) Information Provided to CAC

向网信部门提供的信息

Article 4 lists what needs to be provided by applicants to the CAC. We seek further clarification as noted below:

《评估办法》第 4 条列举了安全评估申报人需要向网信部门提供的材料，我们希望进一步厘清以下问题：

1) For the first item, will CAC publish a standard form of declaration letter?
对于第一项材料，网信部门是否会发布申报书的标准格式？

2) The second piece of information requested is the contract between the Network Operator and the recipient. Investigating contracts signed between parties is time-consuming and impractical, and contractual restrictions relating to disclosure may exist; therefore, we suggest aligning to international practice where the Network Operator summarizes the transfer and terms of the contract. Use of a CAC template contract as mentioned above may ease administrative burdens for all parties here.
第二项材料是网络运营者与接收者签订的合同。对当事人自行签订的合同进行审查十分耗时且不切实际，并且合同中也可能有禁止披露内容的限制；因此，我们建议与国际惯例一致，仅要求网络运营者对传输安排和合同条款进行概述。如果可以按照上述的建议使用网信部门的标准合同，亦可以减轻各方的行政负担。

3) The fourth piece of documentation refers to other materials required by the CAC. This is far-reaching and open ended. Firstly, the provincial CAC is the assessment authority instead of Central Cyberspace Administration Commission; secondly, "other materials" are uncertain and Network Operators may worry about the stability and transparency of the requirements over assessment documentation; we therefore suggest removing such requirement or replacing it with something much clearer.
第四项材料是"国家网信部门要求提供的其他材料"，这一要求过于宽泛。首先，负责安全评估的部门是省级网信部门而非国家网信部门；其次，"其他材料"一词并不明确，网络运营者由此可能对安全评估材料要求的稳定性和透明度产生担忧；因此我们建议删除这一要求或改用更为清晰的表述。

b) Assessment Standard
评估标准

Article 2 provides that the security assessment will be based on whether the data transfer may or may not affect national security or harm the public interest, or that security of personal information is difficult to effectively protect. This is subjective and vague; we would appreciate if CAC could provide

more detail or examples of the scenarios where CAC considers that the outbound transfer would be deemed to have a harmful impact. We would also reiterate that for regulated financial institutions oversight already exists and this should be considered in deciding whether security assessments are needed or whether any assessment can be fast-tracked.

《评估办法》第 2 条规定，安全评估的标准是个人信息出境是否可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全。这一标准过于主观而模糊。我们恳请贵办公室提供更多细节或示例，以说明网信部门在何种情况下会认为个人信息出境将造成有害影响。我们再一次表明：对于受监管金融机构的数据出境，目前已经存在相关的监督。网信部门在决定是否需要对其进行安全评估或是否可以快速进行评估时应当考虑这一因素。

Article 6(2) provides that the security assessment will investigate whether the terms of the contract can fully safeguard the legitimate rights and interests of the personal information subject. As the Outbound Transfer Measures stipulate detailed requirements over the contract as mentioned above, we sincerely suggest rephrasing Article 6(2) into "whether the Contract include the terms as set out in Articles 13 to 16 of these Measures". Once again, relying on the EU Template Contracts in addition to publishing a template Chinese contract (with input from the private sector) may make it operationally easier to comply with Article 6(2).

《评估办法》第 6 条第 2 项规定，安全评估将考虑合同条款是否能够充分保障个人信息主体合法权益。如前述，鉴于《评估办法》对相关合同已经规定了详细要求，我们诚恳地建议将第 6 条第 2 项改为"合同是否包括本办法第 13 条至第 16 条规定的条款"。 我们再次提出，参考欧盟标准合同并在参考行业的意见后发布中国版标准合同，可以让第 6 条第 2 款在实际运行中更易得到遵守。

Members also seek clarification that where a recipient is part of a corporate group which has multiple subsidiaries, a single security assessment in respect of the recipient group will be satisfactory. This will greatly reduce the regulatory burden on day to day business operations.

我们的会员还希望明确，如果接收者实体属于拥有多个子公司的公司集团，则只需对接收者所属的集团进行一次统一的安全评估。这将大大减轻日常业务运营的监管负担。

c) Appeal against the Assessment Results
对评估结果的申诉

Article 7 provides Network Operators with the right of raising an appeal if there is any objection to the result of the security assessment. GFMA members welcome such empowerment and suggest specifying the timeframe of the appeal process. We believe CAC should respond to an appeal within 15 working days of it being raised, to align with the timeframe for the CAC security assessment in Article 5.

《评估办法》第 7 条规定了网络运营者对安全评估结论存在异议时具有申诉权。我们的会员十分欢迎这一安排，同时建议明确申诉过程的时限。我们认为，国家网信部门应在申诉提起后 15 个工作日内进行答复，这亦与《评估办法》第 5 条下安全评估的时限保持一致。

d) Suspension or Termination of Outbound Transfer
暂停或终止向境外提供个人信息

Article 11 provides that under certain circumstances such as relatively serious data breach, CAC may require network operators to suspend or terminate the outbound transfer of the personal information. First, the Outbound Transfer Measures' lack of clarifications regarding when and how the suspension or termination could be applied brings uncertainty with regards to enforcement. Second, we believe that, compared to pure suspension or termination of such outbound transfers, remedies such as implementation of contractual arrangements such as indemnity and/or administrative punishment would be more reasonable and proportionate considering the nature of the breach. Therefore, we would suggest removing this article or otherwise providing more guidance on how this power would work in practice.

《评估办法》第 11 条规定，在特定情况下（例如发生较大数据泄露），网信部门可以要求网络运营者暂停或终止向境外提供个人信息。首先，《评估办法》并未明确该暂停和终止措施会在何时以何种形式执行，可能存在不确定性。其次，我们认为，相比简单暂停或终止向境外提供个人信息，更合理且合适的做法是要求运营者根据合同安排及进行赔偿或进行行政处罚。因此，我们建议删除这一条，或就该权力在实践中如何运行提供更多指引。

7. Transfer Record Keeping
出境记录保存

We fully understand the requirement of Article 8 regarding transfer record keeping, however we seek clarification regarding the details of the requirements. Given the ubiquitous nature of data and ongoing nature and scope of transfers, the record requirements are onerous, especially where it asks for the date and time of the outbound transfer and quantity of personal information. We suggest clarifying that Network Operators are entitled to delete such information and only keep a summary of outbound transfer instead, and to remove the Article 8 (4), i.e. other contents stipulated by CAC, which is open-ended and vague.

我们完全理解《评估办法》第 8 条关于保存个人信息出境记录的要求，但我们希望厘清该要求的细节。鉴于个人信息的广泛性以及传输的持续性，保存出境记录的要求将非常繁重，尤其是对于出境的日期和时间以及个人信息的数量的记录要求。我们建议明确网络运营者仅需保存出境记录的总结，并有权删除被传输的信息本身；此外，我们希望能够删除第 8 条第 4 项"国家网信部门规定的其他内容"这一开放而模糊的要求。

8. Reporting Obligation
报告义务

a) Annual Report
年度报告

According to the first sentence of Article 9, cross-border individual information transfer will be filed with local provincial CAC on an annual basis. We understand it will be more reasonable to request Network Operators to report to sectoral regulators rather than CAC (for example banks could report to CBIRC and / or PBOC).

根据《评估办法》第 9 条第 1 款，个人信息出境情况需要每年报送所在地省级网信部门。我们理解，更合理的做法是要求网络运营者向行业监管部门而非网信部门报告（如银行可报银保监会和/或人民银行）。

We also seek further clarification regarding the contents of annual report; such as if it is a summary of all the data security assessments filed with the CAC or otherwise. If the report needs to cover the information listed in Article 8, it would be burdensome and impractical for Network Operators to perform.

我们还希望进一步明确年度报告的内容，例如它是否是所有已向网信部门提交的安全评估的摘要。如果报告需要涵盖《评估办法》第 8 条所列的全部信息，那么这对于网络运营者而言将是繁重而不具可操作性的要求。

In practice the information that would be reported would not be any different to the information provided under Article 4 and Network Operators could simply provide a declaration that such information is up to date.

实际上，如果该条要求报告的信息和《评估办法》第四条下为安全评估而提供的信息并无区别。那么只需要要求网络运营者声明相关信息是最新的即可。

Members also request clarity that annual reports can be provided three months after the relevant calendar period has ended, to ensure there is enough time to produce any required documentation.

我们的会员还希望明确：年度报告只需要在日历年结束后三个月内报送，以保证运营者有足够时间准备规定的材料。

b) Incident Reporting
临时报告

The second sentence of Article 9 requires Network Operators to promptly report to local provincial CAC when comparatively serious data security incidents happen. We note that in Article 35 of the draft of Administrative Measures on Data Security (《数据安全管理办法》) released in May 2019, if security incidents (i.e. where personal information is divulged, damaged or lost, or the risk of data security incidents has increased significantly) occur, Network Operators shall report to the competent regulatory departments of the industry and CACs in accordance with relevant requirements. We seek to clarify if the "relevant requirement" mentioned in Administrative Measures on Data Security refers to the incident report under this Outbound Transfer Measures, or if there are two sets of reporting obligations. In addition, "comparatively serious data security incidents" is not a defined term and it may therefore cause confusion for Network Operators subject to the reporting obligation. We therefore seek a clear and exercisable definition of "comparatively serious data security incidents."

第 9 条第 2 款要求网络运营者在发生较大数据安全事件时及时报所在地省级网信部门。我们注意到之前在 2019 年 5 月发布的《数据安全管理办法》（征求意见稿）第 35 条规定，发生安全事件（即个人信息泄露、毁损或丢失，或者发生数据安全事件风险明显加大）时，网络运营者应按要求向行业主管部门和网信部门报告。我们希望明确，《数据安全管理办法》中提及的"要求"即是指本《评估办法》规定的安全事件报告，还是有两套报告义务。此外，"较大数据安全事件"并非一个明确的术语，因此可能给负有报告义务的网络运营者带来困惑。因此，我们希望为"较大数据安全事件"提供明确且可执行的定义。

c) Inspections
检查

According to Article 10, the provincial CAC shall regularly organize inspections of outbound transfers of personal information conducted by Network Operators, including the outbound transfer records of personal information, with an emphasis on the fulfillment of contractual obligations, whether there are any violations of national rules or harm to the legitimate rights and interests of data subjects, and other behavior. We believe the inspections and audits on Network Operators should be in relation to the security assessment only, i.e. if security assessment of outbound transfer have been conducted appropriately, then we seek clarification on this point to clearly define the scope of application.

根据《评估办法》第 10 条，省级网信部门应当定期组织检查运营者的个人信息出境记录等个人信息出境情况，重点检查合同规定义务的履行情况、是否存在违反国家规定或损害个人信息主体合法权益的行为等。我们认为对网络运营者的检查和审计应只针对安全评估，即网络运营者是否按照规定进行了数据出境安全评估，因此我们希望贵办公室就检查范围这一问题进行明确。

Article 10 also provides that where any incident occurs, which is detrimental to the legitimate rights and interests of Personal Information subjects or is in relation to security incidents of data leakage, the provincial CAC is entitled to require the Network Operators to rectify. We sincerely request that

definitions or thresholds of "detrimental to the legitimate rights and interests of Personal Information subjects or is in relation to the security incident of data leakage, etc." be provided. We request CAC to specify whether or not it applies only in the context of a cross-border transfer of personal information.

第 10 条还规定，发现损害个人信息主体合法权益、数据泄露安全事件等情况时，省级网信部门有权要求网络运营者整改。我们真诚希望对"损害个人信息主体合法权益、数据泄露安全事件等情况"给出定义或判断标准；亦希望贵办公室明确该条的适用范围仅限于个人信息出境的情形。

9. Contractual Relationship between Data Subjects and Recipients
个人信息主体与接收者间的合同关系

In practice, a data subject will have interactions only with the Network Operator which collected his/her personal data. Creating a direct relationship between that data subject and the data recipient according to the Outbound Transfer Measures, creates a confusion in roles and administrative burden and would not necessarily improve data subjects' rights and interests. This would also potentially allow the data subject to double-claim compensation from both the data recipient and the Network Operator. We therefore suggest the following amendments to the Outbound Transfer Measures:

在实践中，个人信息主体一般仅与收集其个人数据的网络运营者发生往来。如果按照《评估办法》的规定，在个人信息主体与个人信息接收者之间建立直接法律关系会造成角色混乱，增加行政负担，且未必能提升个人信息主体的权益。这还可能使个人信息主体得以从个人信息接收者和网络运营者处进行双重索赔。因此，我们诚挚建议对《评估办法》做出以下修改：

1) *Article 13(2):* deleting the provision that the data subject should be the beneficiary of the contractual terms between the Network Operator and the data receiver.
第 13 条第 2 项：删除"个人信息主体是网络运营者和个人信息接收者间合同条款的受益人"的规定。

The purpose of the contract is for the Network Operator and the recipient to clearly define their respective rights and obligations to each other, with liability for breach of contract applying to them alone.
这些合同的目的是让网络运营者和个人信息接收者明确各自相互的权利和义务,包括相互承担的违约责任。

It is not necessary for the personal data subject to be contracting party to obtain damages in the event they are subject to harm. Under Chinese law, harm to the personal data subject's

non-contractual rights creates tortious liability rather than contractual liability. The personal data subject retains the right to claim damages or compensation for tortious infringement even where it is not a party to a contract.

个人信息主体无需成为合同一方也可以在受损害时得到赔偿。根据中国法律，对个人信息主体的非合同权利的损害会产生侵权责任，而不是合同责任。个人信息主体即使不是合同当事人，也有权就侵权行为主张赔偿或补偿。

2) *Article 13(3):* where a data subject is harmed, he or she should claim compensation only from the original Network Operator that collected their data. That Network Operator will, in turn, contractually ensure that it is indemnified by the data recipient should harm result from the data recipient's acts/omissions. CAC could include such a provision in a template contract.

第 13 条第 3 项：请考虑进行修改，个人信息主体受到损害时，应当仅向最初收集其个人数据的网络运营者主张赔偿。该网络运营者将在合同中相应确保个人信息接收者在其行为/不作为造成损害时承担赔偿责任。贵办公室可以在模板合同中纳入类似条款。

3) Please consider limiting the application of Article 14 to where the transferor collects data directly from the information subject, for the reasons given above.

出于上述原因，也恳请贵办公室考虑将第 14 条的适用范围限缩至直接从个人信息主体处直接收集个人信息的网络运营者。

4) *Article 13*: Large corporate groups usually store data in different locations and have diverse data storage operating procedures across subsidiaries. To be practical, we would suggest CAC clarifying that instead of dozens or possible hundreds of contracts, a single contract between the Network Operator's parent company (or other operating subsidiary) and the recipient's parent company or operating subsidiary be permitted (or such other combination as the parties consider appropriate depending on their circumstances).

第 13 条：大型企业集团通常将数据存储在不同的位置，且各个子公司有不同的数据存储操作规程。从可操作性角度出发，我们建议贵办公室明确，允许网络运营者的母公司（或其他运营子公司）与接收方的母公司或运营子公司之间签订统一合同（或各方视情况认为适当的一组合同），而非逐次签订几十份甚至几百份合同。

5) *Article 14(1) and 16(1):* please consider amending these provisions to state that basic information about the data recipient and the third party shall be described in general terms in the contractual documentation between the data subject and the Network Operator or in the Network Operator's privacy policy. Informing data subjects of specific details of the data recipient/third party for any data transfers would be impractical and costly for organizations;

第 14 条第 1 项、第 16 条第 1 项：请考虑修改这些条款，规定个人信息接收者和第三方的基本信息应在个人信息主体与网络运营者间的合同文档活网络运营者的隐私政策中做一般描述。直接向个人信息主体通报个人信息接收者/第三方的一切个人信息传输的具体细节对于任何机构来说都是不切实际且成本高昂的行为。

6) *Article 14(2)*: please consider deleting the provision that the Network Operator should provide the data subject with a copy of the contract with the data recipient upon data subject's request. Such contracts can be highly confidential and can contain very sensitive information. Disclosing this information to the data subject can pose a serious risk to the security and safety of the data handled and may disclose proprietary information about Network Operator/data recipient's processes and protocols. Mandating a template contract which could be published online may mitigate concerns here.

第 14 条第 2 项：请考虑删除网络运营者应当根据个人信息主体的请求提供与个人信息接收者签订的合同副本的规定。此类合同可能高度保密，并可能包含非常敏感的信息。向个人信息主体披露此信息可能会对所处理信息的安全性构成严重威胁，并可能泄露有关网络运营者/个人信息接收者的经营规程的专有信息。制订一份模板合同并在网络上公开则可以缓解这一问题。

7) *Article 15:* please consider rephrasing the provision to state that the data recipient should provide full assistance in protecting data subjects' rights instead of providing access. Generally, the recipients should not provide the data subject with access to personal data but should be contractually obliged to assist the original Network Operator in such instances. The application of this type of obligation should also depend on the capacity of the recipient (i.e. whether it is acting as a controller rather than a processor).

第 15 条：请考虑修改该条款，规定个人信息接收者应在保护个人信息主体的权利方面提供全面协助，而非提供个人信息的访问途径。通常而言，接收者不应直接向个人信息主体提供对个人信息的访问途径，而应承担协助网络运营者的合同义务。是否适用此类义务还应取决于接收者所承担的角色（即它是否是个人信息控制者而非处理者）。

8) *Article 16(2):* please consider rephrasing the provision such that instructions from the data subject to stop transfer to third parties come through the original Network Operator only. The data subject should not instruct the data recipient directly. In addition, some data recipients may need to retain some personal data for regulatory purposes as banks will be subject to record keeping requirements (e.g. transaction records).

第 16 条第 2 项：请考虑修改该条款，规定个人信息主体请求停止向第三方传输的指令仅应通过原始网络运营者发出。个人信息主体不应直接指示个人信息接收者。此外，一些个人信息接收者可能需要出于监管目的保留一些个人数据，例如银行必须遵守交易记录等记录保留要求。

9) *Article 16:* where the Network Operator obtains personal information through third parties, the Network Operator will not have a direct relationship with the data subject and as a result will not be able to obtain the subject's consent nor notify the subject directly. Therefore, we request further clarification on the meaning and extent of the obligation or responsibilities that should be considered fulfilled in case of no direct relationship with the data subjects. The requirement to notify individuals of the transfer of their data by the recipient to third parties is burdensome and unnecessary to protect their interests. In addition, we seek clarification on whether consent for transfer must be obtained only when Sensitive Personal Information is involved. We also note that Article 27 of the consultation draft of Administrative Measures on Data Security also addresses obtaining consent when transferring personal data to third parties. Please consider reconciliation of these two articles. Moreover, we recommend modifying this article to make it clear that a Network Operator and the third party recipient need to clarify in the contract that the third party must fulfill the same data security protection obligations as the recipient, and that the data security management responsibility cannot be transferred or delegated.

第 16 条：如果网络运营者通过第三方获取个人信息，网络运营者将不会与个人信息主体有直接联系，因此无法获取主体的同意，也无法直接通知主体。因此，我们希望进一步明确在网络运营者与个人信息主体没有直接联系的情况下，网络运营者无需履行该等义务或责任。要求接收者向个人通知其向第三方传输个人信息的行为，对接收者是一项繁重的工作，并且对于保护个人利益必要性不大。此外，我们请求厘清是否只有在涉及传输个人敏感信息时才必须征得同意。我们还注意到，之前的《数据安全管理办法》征求意见稿第 27 条也涉及在将个人信息传输给第三方时征得同意。请考虑协调这两条规定以保持一致。此外，我们建议修改该条，明确规定网络运营者和第三方接收者需要在合同中明确，第三方必须履行与接收者相同的个人信息保护义务，并且个人信息安全管理责任不得转移或委派。

10. Other

其他

Article 17 provides that the report of security risks in personal information outbound transfer and security measures shall include the background, scale, industry, finance, reputation and cybersecurity capabilities of the Network Operator and recipient. We fully understand it is necessary to review the

capabilities of the data recipient, however, we wish to clarify if they will be required to provide supporting documents and make any representations.

《评估办法》第 17 条规定，网络运营者关于个人信息出境安全风险及安全保障措施分析报告应当至少包括网络运营者和接收者的背景、规模、业务、财务、信誉、网络安全能力等。我们完全理解有必要审查个人信息接收者的能力，但是，我们希望明确是否需要个人信息接收者提供证明材料并作出任何陈述。

Article 20 provides that overseas organizations shall fulfill the responsibilities and obligations of Network Operators by domestic legal representatives of organizations. We seek clarification regarding whether Network Operators' duties and responsibilities have to be performed by domestic legal representatives or organizations, as this may create an additional requirement on foreign entities, i.e. to establish local presence, which will have implications such as nature of representation, tax considerations and cross-border payment. We sincerely suggest to further delete this Article because most multi-national companies fulfill their functions and duties at a central level.

《评估办法》第 20 条规定，境外机构应当在境内通过法定代表人或者机构履行网络运营者的责任和义务。我们请求厘清网络运营者的职责和责任是否必须由国内法定代表人或机构履行，因为这可能会对外国实体提出额外的要求——即建立本地业务——并引出诸如国内代表实体的性质、税务考量和跨境支付等问题。我们诚挚地建议删除该条，因为大多数跨国公司都在会在其总部一级集中履行相关职能和职责。

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。

Faithfully,
顺颂时祺,

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
证券业与金融市场协会首席执行官兼主席