COVINGTON

China Seeks Public Comments on Draft Regulation on Cross-Border Data Transfer

April 12, 2017

Data Privacy and Cybersecurity

On April 11, 2017, the Cyberspace Administration of China ("CAC") released a draft of the *Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data* ("the Draft Measures") for public comment (official Chinese version available here; Covington's translation of the Draft Measures is appended at the end of this alert). The comment period ends on May 11, 2017.

The issuance of the long-anticipated Draft Measures is another critical step toward implementing China's *Cybersecurity Law* ("the Law"), which is set to take effect on June 1, 2017 (see Covington alert on the Law here). Importantly, the Draft Measures, if enacted in their current form, would mandate all "network operators" to self-assess the security of their cross-border data transfers and significantly broaden the scope of entities that potentially need to undergo security assessments for such transfers by the Chinese government. Companies that fall into the scope of "network operators," but may not qualify for "operators of Critical Information Infrastructure" ("CII"), could see their cross-border data transfers regulated under the Draft Measures.

Given the potentially sweeping coverage of the Draft Measures, companies seeking to transfer Chinese citizens' personal information and "important data" outside of China should consider taking steps to proactively self-assess their cross-border data flows and be prepared for the government's security assessment if the Draft Measures are enacted as they are drafted now.

Background

Before the Law was officially promulgated, China had already begun consolidating its jurisdiction over data by imposing data localization requirements in many industry-specific regulations. However, there existed no comprehensive framework for regulating cross-border data flows.

Article 37 of the Law, for the first time, expressly requires that operators of CII store within China "citizens' personal information and important data" collected or generated in the course of operations within the country. If transfers of data offshore are necessary for operational reasons, a security assessment must be conducted by designated agencies, unless laws and regulations specify otherwise.

Expansive Scope of Regulated Entities

Although released as an implementing regulation of the Law, the Draft Measures significantly expand the scope of entities for which cross border data flow may be regulated.

Under Article 37 of the Law, if a company is not deemed as an operator of CII, its cross-border data flows will not be regulated. However, the Draft Measures replaced "operators of CII" (from Article 37 of the Law) with "network operators" (Article 2).

The term "network operators" is defined as "owners and managers of networks, as well as network service providers" (Article 17). This definition is consistent with the definition provided by Article 76 (3) of the Law. In the first draft of the Law issued in 2015, "network operators" were described to include operators of "basic telecommunication networks, internet information service providers, and key information system operators." Such a description was later removed from the final version of the Law. As a result, the scope of "network operators" could be expanded significantly to cover every entity that is using a network (including the Internet) to operate or provide services. It is uncertain how expansively CAC and other regulators will interpret this term to cover companies that are only using networks, but are not either operators of "basic telecommunication networks, internet information service providers, and key information system operators," or "operators of CII."

Substantive Criteria of Security Assessment

The Draft Measures provide that the overriding principles for the security assessment of cross-border data transfer are "fairness, objectivity, and effectiveness" (Article 3). The security assessment should also promote "lawful, orderly, and free" flow of information.

More specifically, the security assessment should focus on the following aspects of cross-border data transfers (Article 8):

- Necessity of such transfers;
- Amount, scope, type, level of sensitivity of personal information involved, and whether data subjects have consented to such transfers;
- Amount, scope, type, level of sensitivity of important data involved;
- Data recipients' data security measures, capabilities, and their level of protection, as well as the cybersecurity environment of the countries or regions in which the recipients are located;
- Risks arising from cross-border transfers or subsequent re-transfers of data in terms of such data being leaked, damaged, tampered with, or misused; and
- Risks posed by cross-border data transfers (including the aggregation of data transferred to offshore locations) to China's national security, societal and public interests, and Chinese citizens' rights and interests.

Cross-border data transfers will be prohibited in any of the following circumstances (Article 11):

- Data subjects do not consent to the transfer of personal information, or if such a transfer may cause harm to the data subject's rights and interests;
- The transfer poses risks to China's national security or public interests; or
- Other circumstances in which the Chinese government determines that the data concerned is prohibited from being transferred offshore.

Self-assessment and Government Security Assessment

The Draft Measures provide that "network operators" are all required to organize their own security assessment for cross-border data transfers and are responsible for the results of such self-assessments (Article 7).

An industry regulator will conduct a security assessment of the following data transfers (Article 9):

- Transfers (individually or accumulatively) of personal information of over 500,000 Chinese citizens;
- Transfers exceeding 1,000 gigabytes;
- Transfers involving data regarding "nuclear facilities, chemical biology, national defense or military, population and health care, etc.," and data related to "large-scale engineering activities, marine environment, and sensitive geographic information";
- Transfers involving data related to cybersecurity information of China's CII operators, such as their system vulnerabilities or security measures;
- Transfers involving the provision of personal information and important data to overseas recipients by operators of CII; and
- Other transfers that may potentially affect China's national security and public interests.

Transfer of Personal Information

The Draft Measures provide that where personal information is to be transferred offshore, data subjects must be notified of "the purpose, scope, content, the recipient of the transfer, as well as the country or region in which the recipient is located," and the data subjects must give their consent (Article 4). Also, if the personal information to be transferred concerns a minor, the consent of the guardian must be obtained.

Consistent with the Law, "personal information" is defined by the Draft Measures to include "various types of information recorded by electronic or other means that can, independently or in combination with other information, identify a natural person, including but not limited to a natural person's name, date of birth, identity certificates numbers, personal biological identification information, address and telephone numbers" (Article 17).

Based on this provision and other requirements for security assessments of cross-border data transfer, in addition to consent, transfer of personal information outside of China will likely have to rely on network operators' commitments or binding contractual obligations to ensure that personal information is sufficiently protected outside of China.

Dual Enforcement Structure

Under the Draft Measures, CAC will be responsible for policy-making and coordination between industry regulators with respect to the overall security of cross-border data transfers (Article 5). Industry regulators will be responsible for conducting security assessments in their respective sectors (Article 6). If an industry regulator cannot be identified, the security assessment can be organized by CAC (Article 9).

Security Assessment Process

Security assessments conducted by industry regulators shall be completed within 60 working days. The agencies should provide timely feedback to network operators and inform CAC of the results (Article 10).

After the initial assessment, network operators should undergo annual self-assessment and report the results to the industry regulators (Article 12).

If there is a change in circumstances, for example, a different data recipient, or a significant change in the purpose, scope, amount, or type of data transferred offshore, or if there is a material security incident involving the data recipient or the data to be transferred, the security assessment must be conducted again promptly (Article 12).

Penalty

Article 14 vaguely states that entities violating provisions in the Draft Measures will be punished "in accordance with relevant rules and regulations." Note that Article 66 of the Law specified penalties for operators of CII which violate Article 37 of the Law by storing or transferring data offshore illegally. The Law, however, does not provide a similar penalty provision for network operators violating cross-border data transfer requirements.

International Agreement

Article 15 provides that if China signs agreements with other countries or regions relating to cross-border data transfer, such agreements shall prevail, *except* where national secrets are involved. This leaves open the possibility of data transfer agreements between China and other countries, even though CAC has not provided any details on how it plans to evaluate whether foreign countries are willing and capable of safeguarding Chinese data post-transfer.

Conclusion

Although the Draft Measures furnish some basic parameters of the security assessment of cross-border data transfer, the meaning and scope of many of the Draft Measures' provisions are unclear. In particular, the Draft Measures' expansive interpretation on covered entities creates tremendous uncertainties for companies that may be considered as unregulated under the Law.

In managing these uncertainties, companies may consider steps to clarify their status with industry regulators, while self-assessing their cross-border data transfers and preparing for government assessments if they are later confirmed as regulated entities.

If you have any questions concerning the material discussed in this client alert or would like to comment on the Draft Measures, please contact any of the following members of our firm:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com

Covington Unofficial Translation

个人信息和重要数据出境安全评估办法

Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data

（征求意见稿）

(Draft for Comments)

第一条 为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

Article 1 In order to protect the security of personal information and important data, to safeguard the cyberspace sovereignty, national security, societal and public interests, and to protect the lawful rights and interests of citizens, legal persons and other organizations, these Measures are formulated in accordance with the National Security Law of the People's Republic of China and the Cybersecurity Law of the People's Republic of China.

第二条 网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

Article 2 Personal information and important data collected and generated in the course operation of network operators within the territory of the People's Republic of China shall be stored within the territory. If it is necessary to provide such information and data overseas for operational reasons, a security assessment shall be conducted in accordance with these Measures.

第三条 数据出境安全评估应遵循公正、客观、有效的原则，保障个人信息和重要数据安全，促进网络信息依法有序自由流动。

Article 3 The security assessment of the cross-border data transfer shall abide by the principles of fairness, objectiveness and effectiveness to protect the security of personal information and important data and promote the lawful, orderly, and free flow of network information.

第四条 个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

Article 4 For cross-border transfer of personal information, personal information data subjects shall be notified regarding the purpose, scope, content, the recipient, as well as the country or region in which the recipient is located, and shall consent to the transfer. The cross-border transfer of personal information of a minor must be consented by the guardian.

第五条 国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估。

Article 5 The national cyberspace authority shall be responsible for overall coordination of work in connection with the security assessments of cross-border data transfers and shall guide competent industry regulators or regulatory authorities in organizing the security assessments of cross-border data transfers.

第六条 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。

Article 6 Competent industry regulators or regulatory authorities shall be responsible for the work of security assessments of cross-border data transfers in their respective industries and shall organize to carry out security inspections of cross-border data transfer in their respective industries at regular intervals.

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。

Article 7 Network operators shall organize self-assessment for the security of cross-border data transfer before the data is transferred overseas and shall be responsible for the results of such an assessment.

第八条 数据出境安全评估应重点评估以下内容：

Article 8 The security assessment of the cross-border data transfer shall focus on the following aspects:

(1) 数据出境的必要性；
(1) The necessity of the cross-border data transfer;

(2) 涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；
(2) The personal information involved, including, among others, the amount, scope, type, level of sensitivity, and whether the data subject has consented to the cross-border transfer of personal information;

(3) 涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；
(3) The important data involved, including, among others, the amount, scope, type, level of sensitivity of the important data;

(4) 数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；
(4) The data recipient's security measures, security capability, and level of security protection, as well as the cybersecurity environment of the country or region in which the recipient is located;

(5) 数据出境及再转移后被泄露、毁损、篡改、滥用等风险；
(5) The risks arising from the data being leaked, damaged, tampered with or misused after cross-border data transferor subsequent re-transfer.

(6) 数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；
(6) The risks posed to national security, societal and public interests, and individual lawful rights and interests arising from the cross-border transfer and aggregation of data.

(7) 其他需要评估的重要事项。
(7) Other important aspects that must be assessed.

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：
Article 9 If any of the following conditions applies to the data to be transferred overseas, the network operator shall file with the competent industry regulator or regulatory authority to organize the security assessment:

(1) 含有或累计含有 50 万人以上的个人信息；
(1) Contains or accumulatively contains personal information of more than 500,000 individuals;

(2) 数据量超过 1000 GB；
(2) The amount of data exceeds 1,000 GB;

(3) 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；
(3) Contains data regarding, for example, nuclear facilities, chemical biology, national defense or military, population health, data related to large-scale engineering activities, the marine environment, and sensitive geographic information;

(4) 包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；
(4) Contains cybersecurity information such as system vulnerabilities or security measures relating to critical information infrastructure;

(5) 关键信息基础设施运营者向境外提供个人信息和重要数据；
(5) Provision of personal information and important data to overseas recipients by operators of Critical Information Infrastructure;

(6) 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。

(6) Other circumstances that possibly affect national security and societal and public interests that are considered to be subject to assessment by the competent industry regulators or regulatory authorities.

行业主管或监管部门不明确的，由国家网信部门组织评估。
If the competent industry regulators or regulatory authorities are unclear, the assessment shall be organized by the national cyberspace authority.

第十条 行业主管或监管部门组织的安全评估，应当于六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。
Article 10 The security assessment organized by competent industry regulators or regulatory authorities shall be completed within 60 working days. The competent industry regulator or regulatory authority shall provide network operator with feedback on the security assessment result timely and shall file the result with national cyberspace authority.

第十一条 存在以下情况之一的，数据不得出境：
Article 11 Data is prohibited from being transferred overseas in any of the following circumstances:

(1) 个人信息出境未经个人信息主体同意，或可能侵害个人利益；
(1) The personal information data subject does not consent to the cross-border transfer of personal information, or if such transfer may cause harm to personal rights and interests;

(2) 数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；
(2) The cross-border data transfer will pose risks to the security of the nation's politics, economy, technology, or national defense, and therefore may affect national security or damage societal and public interests;

(3) 其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。
(3) Other circumstances in which the national cyberspace, public security, security, or other relevant departments determine that the data concerned is prohibited from being transferred overseas.

第十二条 网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报行业主管或监管部门。
Article 12 Network operators shall, based on business development and network operations, conduct a security assessment of cross-border data transfer at least once a year and shall report the assessment results in a timely fashion to the competent industry regulator or regulatory authority.

当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。
If the recipient of data is changed or there is significant change on the purpose, scope, amount, types of the cross-border data transfer or there is material security incident regarding the data recipient or the data to be transferred overseas, the security assessment shall be re-conducted in a timely fashion.

第十三条 对违反相关法律法规和本办法向境外提供数据的行为，任何个人和组织有权向国家网信部门、公安部门等有关部门举报。
Article 13 Any individual or organization has the right to report to the relevant department, such as the national cyberspace authority and public security department, with respect to any activities of providing data overseas that are in violation of relevant laws and regulations and these Measures.

第十四条 违反本办法规定的，依照有关法律法规进行处罚。
Article 14 Whoever violates any provisions of these Measures shall be punished in accordance with relevant laws and regulations.

第十五条 我国政府与其他国家、地区签署的关于数据出境的协议，按照协议的规定执行。
Article 15 Where there are any agreements between the Chinese Government and other countries or regions relating to cross-border data transfer, those agreements shall prevail.

涉及国家秘密信息的按照相关规定执行。
If national secrets are involved, relevant provisions shall prevail.

第十六条 其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。
Article 16 The work of security assessment of cross-border transfer of personal information and important data collected and generated by other individuals and organizations within the territory of the People's Republic of China shall be implemented with reference to these Measures.

第十七条 本办法下列用语的含义：
Article 17 The following terms in these Measures shall have the following meanings:

网络运营者，是指网络的所有者、管理者和网络服务提供者。
"Network operator" means the owner or manager of the network and network service provider.

数据出境，是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。

“Cross-border data transfer” means that network operators provide overseas institutions, organizations, or individuals with personal information and important data collected and generated within the territory of the People’s Republic of China.

个人信息，是指以电子或者其他方式记录的能够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，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。
“Personal information” means various types of information recorded by electronic or other means that can, independently or in combination with other information, identify a natural person, including but not limited to a natural person’s name, date of birth, identity certificate numbers, personal biological identification information, address and telephone numbers.

重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。
“Important data” means data closely related to national security, economic development and societal and public interests. The specific scope of the important data shall be determined with reference to relevant national standards and guidelines on important data identification.

第十八条 本办法自 2017 年 月 日起实施。
Article 18 These measures shall come into effect as of [*date*] 2017.