COVINGTON

China Releases Near-final Draft of Regulation on Cross-border Data Transfers

May 19, 2017

Data Privacy and Cybersecurity

On May 19, 2017, the Cyberspace Administration of China ("CAC") invited international stakeholders to attend a seminar to discuss an updated version of the *Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data* ("the Measures"). (Covington's translation of the Measures is appended at the end of this alert. Amendments to the previous version of the Measures in redline.) A previous draft of the Measures was released for public comments on April 11, 2017. (Covington's alert on the previous version is available here.)

Given that the Measures have an intended effective date of June 1, 2017, it is likely that they are in final form and the framework established by the Measures will govern China's cross border data transfers going forward. This alert summarizes the key changes from the previous version.

Under the Measures, "network operators" in China could face a general obligation to assess the security of their cross data transfers and potentially undergo security assessments for such transfers by the Chinese government, if certain conditions are met. Such an assessment is no longer linked with the status of "operators of Critical Information Infrastructure" ("CII") and a reference to the data localization requirements is removed. Thus, unless the security assessment reveals major risks, companies seeking to transfer Chinese citizens' personal information and "important data" outside of China can continue their practices.

To avoid any disruption of data transfers, companies should consider taking steps to comply with this general obligation of assessing the security of their cross-border data flows and be prepared for the government's security assessment, if and when required.

Reference of Data Localization Removed (Article 2)

As background, Article 37 of the Cybersecurity Law ("the Law") expressly requires that operators of Critical Information Infrastructure ("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.

The previous version of the Measures expanded the scope of Article 37 by mandating that "network operators" store within China "citizens' personal information and important data"

collected or generated in the course of operations within the country. This reference to data localization requirements is removed from the current version. Instead, the Measures, as the text currently reads, focus only on the security assessment of cross border data transfers.

It is uncertain whether other implementing regulations of the Law will still mandate data localization, implementing the requirements under Article 37.

General Obligations for Security Assessment (Article 6) and Regulator Security Assessment (Article 7)

Consistent with the previous version of the Measures, "network operators" are generally obliged to conduct security assessments for their cross-border data transfers in order to "protect public interests and uphold [China's] national security" (Article 6). The explicit call for self-assessment is however removed.

An updated Article 7 requires industry regulators to conduct a security assessment of the following transfers:

- Transfers containing personal information of over 500,000 Chinese citizens;
- Transfers involving:
  - Data regarding "nuclear facilities, chemical biology, national defense or military, population and health care, etc.;"
  - Data related to "large-scale engineering activities, marine environment, and sensitive geographic information;" and
  - Data related to cybersecurity information of China's CII operators, such as their system vulnerabilities or security measures;
- Other transfers that may potentially affect China's national security and public interests.

This new provision removes two criteria from the previous version: "transfers exceeding 1,000 gigabytes" and "transfers involving the provision of personal information and important data to overseas recipients by operators of CII." Also, the reference to data transfers that accumulatively contain personal information of over 500,000 Chinese citizens is removed, even though this modification of the wording will unlikely have practical impacts.

The scope of entities for which cross border data flow may be regulated under the current version of the Measures may be reduced due to the change of wording. However, a sufficient large amount of companies may still find that their data transfers outside of China will be subject to regulators' scrutiny going forward.

Transfer of Personal Information: Exception of Consent and Implicit Consent (Article 4)

Consistent with the previous version, consent remains the most important element for cross border data transfer of personal information in the Measures.

The previous version required 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 that the data subjects must give their consent. In the current version, Article 4 still requires consent to allow cross border data transfers, but the scope of the consent is slightly modified to include "the purpose, scope, type, as well as the country or region in which the recipient is located."

More importantly, the current version provides (i) an exception to the consent rule and (ii) circumstances under which consent can be inferred.

The exception involves transfers that would be "necessitated by an emergency that could endanger the lives and property of [Chinese] citizens [if the data is not transferred]."

The circumstances that consent can be inferred include "making international phone calls, sending emails or instant messages to individuals or organizations overseas, and making cross-border e-commerce transactions," as well as other activities initiated by data subjects.

Substantive Criteria of Security Assessment (Articles 8 and 9)

The substantive criteria of the security assessment remain largely the same in the current version.

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

- Lawfulness, legitimacy, and 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;
- 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 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 9):

- If the transfer does not comply with laws or regulations;
- Data subjects do not consent to the transfer of personal information;
- The transfer poses risks to China's national security or public interests;
- The transfer has the potential of endangering China's security of "national politics, territory, military, economy, culture, society, technology, information, ecological environment, resources, nuclear facilities and so on;" or
- Other circumstances in which the Chinese government determines that the data concerned is prohibited from being transferred offshore.

Process and Result of Regulator Security Assessment (Article 10)

The current version of the Measures still requires that the agencies that are conducting the security assessment should provide timely feedback to network operators (Article 10). But the reference to a 60 working day review period is removed.

As a result, the current version lacks clarity with respect to the procedural steps of the security assessment, including how and when a regulator can initiate an assessment process and how long that review will last.

Under the Measures, a security assessment could result in either the approval of the transfers, which means that the network operator can continue its transfers, or transfers being blocked if any circumstances mentioned in Article 9 is discovered (Article 10).

Effective Dates and Grace Period

The Measures are intended to take effect on June 1, 2017, the same effective date as for the Law. After taking effect, the Measures will provide a grace period of 18 months for companies to comply with the rules and enforcement will start after December 31, 2018.

For more information on this alert, please contact any of the below Covington lawyers:

If you have any questions concerning the material discussed in this client alert, please contact 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

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~~修改稿）

(Revised 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 网络运营者向境外提供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~~（以下称数据出境），应当按照本办法进行安全评估。

法律、行政法规另有规定的，依照其规定。

Article 2 ~~Personal~~When network operators provide 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~~ overseas (hereinafter referred to as cross-border data transfer), a security assessment shall be conducted in accordance with these Measures.

Where laws and regulations provides otherwise, such provision shall prevail.

第三条 数据出境安全评估应遵循公平、公正、客观、~~有效~~透明的原则，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, impartiality, objectiveness and ~~effectiveness~~ transparency to protect the

security of personal information and important data and promote the lawful, orderly, and free flow of network information.

第四条 网络运营者向境外提供个人信息~~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~~类型，以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~~出现危及公民生命财产安全的紧急情况除外。

拨打国际电话、发送国际电子邮件、进行国际即时通信、通过互联网进行跨境交易，以及其他个人主动行为视为已经个人信息主体同意。

Article 4 ~~For cross-border transfer of~~When network operators provide personal information overseas, personal information data subjects shall be notified regarding the purpose, scope, ~~content, the recipient, as well as~~type and the country or region in which the recipient is located, and shall consent to the transfer except the occurrence of urgent circumstances under which the security of citizens' lives and properties are endangered. ~~The cross-border transfer of personal information of a minor must be consented by the guardian~~

Making international phone calls, sending international emails, conducting international instant messaging, conducting cross-border trading through internet and other active behaviors shall be deemed that the consent from personal information subject has been obtained.

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。~~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。

国家网信部门统筹协调指导数据出境安全评估工作。

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.~~ 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.

The national cyberspace authority shall be responsible for overall coordination guidance regarding 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~~网络运营者根据数据出境的类型、数量、重要程度等，对数据出境进行安全评估，保障公众利益、维护国家安全。

当数据出境目的、范围、类型、数量等发生较大变化，数据接收方变更或发生重大安全事件时，应及时进行安全评估。

Article 6 Network operators shall conduct security assessments of cross-border data transfers according to the types, amount and importance of the cross-border data transfer.

~~**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.~~ When the purpose, scope, type and amount of the cross-border data transfer is changed greatly or data recipient is changed or material security incidents happens, security assessment shall be conducted promptly.

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~~出境数据存在以下情况之一的，应当由行业主管或监管部门组织安全评估，~~并对评估结果负责~~行业主管或监管部门不明确的，由国家网信部门组织评估。

Article 7 ~~Network operators~~If any of the following conditions applies to the data to be transferred overseas, the competent industry regulator or regulatory authority 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~~the security assessment. If the competent industry regulators or regulatory authorities are unclear, the assessment shall be organized by the national cyberspace authority.

(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) 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、敏感地理信息数据，以及关键信息基础设施的安全缺陷、具体安全防护措施等网络安全信息；

(2) Contains network security information regarding, nuclear facilities, chemical biology, national defense or military, population health, data related to large-scale engineering activities, the marine environment, and sensitive geographic information and security defects of critical information infrastructure, specific security protection measures;

(3) 其他可能影响国家安全和社会公共利益的。

(3) Other circumstances that possibly affect national security and societal and public interests.

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) 数据出境的合法性、正当性、必要性；

(1) The legality, legitimacy and 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、措施和~~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, measures and ~~level of security protection, as well as the cybersecurity environment of the country or region in which the recipient is located~~environment;

(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~~后可能对国家安全、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~~after 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~~经评估，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~~数据不得向境外提供：

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:~~ Subject to the assessment, data is prohibited from being transferred overseas in any of the following circumstances:

~~(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) 不符合国家法律、行政法规、部门规章等有关规定的；

(1) The cross-border data transfer is in violation of relevant provisions of state laws, administrative regulation, departmental rules;

(2) 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~~2) 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~~;

(3) 可能损害公众和国家利益的个人信息出境；

(3) The cross-border data transfer will damage public and national interests;

(~~2~~4) 数据出境~~给~~危害国家政治、国土、军事、经济、文化、社会、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~~信息、生态、资源、核设施等安全；

(~~2~~4) The cross-border data transfer will ~~pose risks to~~endanger the security of ~~the nation's~~national politics, territory, military, economy, culture, society, technology, ~~or national defense, and therefore may affect national security or damage societal and public interests;~~information, eco logical environment, resources, nuclear facilities and etc.

~~(3)~~(5) 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~~5) 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.~~

第十条 行业主管或监管部门组织的安全评估，应及时向网络运营者反馈安全评估情况，发现有第九条所列情况的，应及时要求网络运营者停止数据出境。

Article 10 For security assessment organized by competent industry regulators or regulatory authorities, the competent industry regulator or regulatory authority shall provide network operator with feedback on the security assessment result timely and shall require network operators to stop the cross-border data transfer timely if the circumstances listed in Article 9 are found. .

~~第十三条~~第十一条 对违反相关法律法规和本办法向境外提供个人信息和重要数据的行为，任何个人和组织有权向国家网信部门、公安部门、安全部门等有关部门举报。

Article ~~13~~11 Any individual or organization has the right to report to the relevant department, such as the national cyberspace authority and public security department, security

department with respect to any activities of providing personal information and important data overseas that are in violation of relevant laws and regulations and these Measures.

第十四二条 违反本办法规定的，依照有关法律法规进行处罚。

Article 1412 Whoever violates any provisions of these Measures shall be punished in accordance with relevant laws and regulations.

第十五三条 我国政府与其他国家、和地区、国际组织签署的关于条约、协议等涉及数据出境的协议，按依照协议的其规定执行。

Article 1513 Where there are any treaties or agreements between the Chinese Government and other countries orand regions or international organizations relating to cross-border data transfer, those treaties and agreements shall prevail.

第十四条 涉及国家秘密信息的按照相关依照保密法律、行政法规的规定执行。

Article 14 If national secrets are involved, relevant provisions in relevant secrecy laws and administrative regulations 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.~~

第十七五条 本办法下列用语的含义：

Article 1715 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~~将电子形式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~~providing information and important data in electronic form to 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或者反映特定自然人活动情况的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、通信通讯联系方式、个人生物识别信息、住址、~~电话号码~~账号密码、财产状况、位置和行为信息等。

"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 or reflect the activity of certain natural person, including but not limited to a natural person's name, date of birth, identity certificate numbers, correspondence and communication contact information, personal biological identification information, address ~~and telephone numbers~~, account number and password, status of property, location and activity information.

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~~六条 本办法自 2017 年 6 月 1 日起实施。

2018 年 12 月 31 日起，网络运营者数据出境应符合本办法要求。

Article ~~18~~16 These measures shall come into effect as of ~~[*date*]~~June 1, 2017.

All cross-border data transfers made by network operators shall conform to these Measures starting from December 31, 2018.