JUNHE BULLETIN

JUNHE

April 12, 2017

# Telecommunication Law

## *Cross-border Data Transfer Assessment Measures* Released for Public Comment

### I. Background

The Cyberspace Administration of China ("**CAC**") released a draft of the *Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data* (the "**Draft**") on April 11, 2017 allowing for one month of public comments to be offered.

Security assessments on the cross-border transfer of personal information and important data was first introduced into law by the Cybersecurity Law (the "**CSL**"), issued in November last year and to become effective on June 1, 2017. The CSL grants the national cyberspace administration the authority to develop security assessment measures in conjunction with other regulatory authorities. Together with the National Security Law, such provisions in the CSL serve as the legal basis for the Draft.

### II. What Data must be Localized?

The Draft extends the requirements for data localization and security assessments on critical information infrastructure operators ("**CIIO**") provided under the CSL to all "network operators", and requires personal information and important data collected and produced by network operators in the course of their operations within China to be stored within the territory of China. Where it is indeed necessary to provide such information and data to overseas parties due to business needs, security assessments must be conducted. (*Article 2*)

The Draft adopts a definition of "personal information" which is similar to the definition in the CSL. For "important data", which is left undefined under the CSL, the Draft provides a broad and ambiguous definition, as "data closely related to national security, economic

development and public interests", and leaves its specific scope to be further stipulated under relevant national standards and identification guides to be formulated. (*Article 17*)

## III. How to Carry Out Assessments?

The Draft regulates cross-border transfers by way of both so-called self-assessments and assessments by authorities. In brief, network operators are required to carry out self-assessments for all cross-border transfers of data (*Article 7*), while for cross-border transfers of data satisfying certain tests, network operators must submit to their industrial regulatory authority or the national cyberspace authority for assessments (*Article 9*).

Such criteria include, for example, the transfer involving or cumulatively involving personal information of more than 500,000 individuals, or having a data volume of more than 1000GB, or the data to be exported includes data in relation to the areas of nuclear facilities, chemistry and biology, national defense and military, health of the population, and data of mega project activities, ocean environment, sensitive geographical information, and again leaves a catch-all provision providing "other situations which may affect national security and societal public interests, and the industrial administration authority or regulatory authority considers the export data should be subject to the security assessment". (*Article 9*)

Network operators shall conduct security assessments of data exports at least once a year and where significant changes occurs to certain aspects of the data exported, re-assessments are required to be carried out. (*Article 12*)

## IV. What is to be Assessed?

The assessment of data exports are to be focused on the following aspects:

- necessity of the data export;
- the amount, scope, type, sensitivity of personal information and important data and individuals' consent in case of personal information;
- security conditions of the recipient and the receiving country;
- possibility of the data being divulged, damaged, tampered with or misused;
- risks for national security, public interest and individual's legitimate interests; and
- other important aspects that need to be evaluated. (*Article 8*)

Data should not be exported if:

- the concerned individual has not consented to the export or his/her interests are jeopardized;
- national security or public interests may be endangered, or
- circumstances prohibited by the competent authorities in their discretion. (*Article 11*)

## V. Observations

Compared to the CSL, the Draft expands the scope of entities subject to data localization and security assessment obligations, and imposes a wide assessment (either self-assessment or government assessment) obligation on network operators, while specific and detailed standards, procedures,

requirements are still to come. Once issued and implemented, the Draft may have extensive impact on the operation and IT structure of companies with cross-border operations in such a fast-developing digitalized world. We will continue to monitor how the Draft will be coordinated with the existing legal system, e.g., regulations on domestic storage or restrictions on cross-border transfer in existing laws and regulations, and how the cooperation between the cyberspace authorities and industrial regulatory authorities is handled.


| | | | |
|---|---|---|---|
| Marissa DONG | Partner | Tel: 86 10 8519 1718 | Email:dongx@junhe.com |
| Kemeng CAI | Associate | Tel: 86 10 8519 1255 | Email:caikm@junhe.com |
| Jinghe GUO | Associate | Tel: 86 10 8553 7947 | Email:guojh@junhe.com |

君合研究简讯

JUNHE

2017 年 4 月 12 日

# 电信与互联网法律热点问题

## 《个人信息和重要数据出境安全评估办法》公开征求意见

### 一、背景

国家互联网信息办公室（以下简称“**网信办**”）于 2017 年 4 月 11 日公布了《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称“**《草案》**”）向社会公开征求意见，截止时间为一个月。

去年 11 月颁布、将于 2017 年 6 月 1 日生效的《中华人民共和国网络安全法》（以下简称“**《网安法》**”）首次在法律中确立了对个人信息及重要数据出境的安全评估制度。《网安法》授权国家网信部门会同其他监管部门制定详细的安全评估实施办法。《网安法》下的这一规定与《中华人民共和国国家安全法》共同构成了《草案》的法律基础。

### 二、什么数据必须本地化

《草案》将数据本地化及安全评估的义务主体从《网安法》规定的“关键信息基础设施运营者”扩展到所有的网络运营者，并要求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，应当进行安全评估。（第二条）

对于个人信息，《草案》采取了与《网安法》类似的定义。对于《网安法》未进行界定的“重要数据”，《草案》采取了宽泛、模糊的定义：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，具体范围参照未来制定的国家有关标准和重要数据识别指南。（第十七条）

### 三、如何进行评估

《草案》通过所谓自行评估及监管机构评估的方式对数据出境进行监管。简要来说，网络运营者需对所有数据出境进行自行评估（第七条），而对满足相应条件的数据出境，网络运营者需报告行业监管部门或国家网信部门进行评估（第九条）。

需进行监管机构评估的情况包括：出境数据含有或累计含有 50 万人以上的个人信息；数据量超过 1000GB；包含核设施、化学生物、国防军工、人口健康等领域的数据；大型工程活动、海洋环境以及敏感地理信息数据等。同时还包括了一个兜底性条款：“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”。（第九条）

网络运营者每年应对数据出境至少进行一次安全评估；当数据出境的相关方面出现较大变化时，应重新进行安全评估。（第十二条）

## 四、评估的内容是什么

数据出境安全评估应重点评估以下内容：

1、 数据出境的必要性；

2、 个人信息及重要数据的数量、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；

3、 数据接收方的安全状况及所在国家；

4、 数据被泄露、毁损、篡改、滥用等风险；

5、 对国家安全、社会公共利益、个人合法利益带来的风险；以及

6、 其他需要评估的重要事项。（第八条）

存在以下情况之一的，数据不得出境：

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；

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；

3、 其他经国家有关部门认定不能出境的。（第十一条）

## 五、简评

与《网安法》相比，《草案》扩大了数据本地化及安全评估义务适用对象的范围，并且对网络运营者施加了广泛的评估义务（自行评估或监管机构评估），但相关明确、具体的标准、程序、要求尚未出台。

在这样一个数字化迅速发展的世界，《草案》发布及实施后，可能对跨境运营公司的运营及 IT 结构产生广泛影响。《草案》与现有法律制度的衔接（例如现有法律法规之中存在境内存储或出境限制的特别规定）、网信主管部门与行业主管部门的对接和配合，也待在实践中进一步观察。

董　潇　合伙人　电话：86 10 8519 1233　邮箱地址：dongx@junhe.com
蔡克蒙　律　师　电话：86 10 8519 1255　邮箱地址：caikm@junhe.com
郭静荷　律　师　电话：86 10 8553 7947　邮箱地址：guojh@junhe.com