JUNHE BULLETIN

JUNHE

June 2, 2017

Telecommunication Law

Guidelines for Cross-Border Data Transfer Security Assessment Released for Public Comment

The National Information Security Standardization Technical Committee ("**TC 260**") released a draft of the *Information Security Technology-Guidelines for Cross-Border Data Transfer Security Assessment* (the "**Guidelines**") on May 27, 2017 allowing for one month of public comments to be offered.

I. Background

The Cyberspace Administration of China ("**CAC**") has released a draft of the *Measures for Security Assessment of the Cross-Border Transfer of Personal Information and Important Data* (the "**Assessment Measures**") on April 11. As an important ancillary implementation regulation of the Cybersecurity Law ("**CSL**"), the Assessment Measures establish the basic framework for security assessment for data exports. According to the Assessment Measures, where the network operators provide personal information and important data collected and generated in the course of operations within the territory of China to overseas parties, security assessments shall be carried out. Security assessments for data exports include both self-assessments and assessments by authorities. On the basis of the Assessment Measures, the Guidelines specifies the requirements for the assessment process, the focus of assessment, assessment methods and the scope and types of "important data" in different sectors and industries.

II. Application

The Guidelines apply to security assessments carried out by network operators. It also applies to the competent industry regulators or regulatory authorities in their guidance and supervision of the security assessments carried out by network operators. The CAC and the competent industry regulators or regulatory authorities may make reference to the Guidelines in the security assessments of data exports carried out within their respective authorities.

III. Security Assessment Process

In accordance with the Guidelines, the security assessment process includes the following steps: initiating self-assessments, formulating data export plans, assessments of the lawfulness, appropriateness and controllability of the data export plans, generating assessment reports, and checks and revisions, etc.

Network operators shall formulate data export plans if their products and services involve the export of data. The data export plans shall include without limitation (1) the destination, scope, type and scale of the data export; (2) the information systems involved; (3) the transit country or region (if any); (4) the basic situation of the receiving party and the country or region where it is located; and (5) security control measures. Network operators shall assess whether the data export plan is lawful, appropriate and controllable by referring to the assessment methods set out in Appendix B of the Guidelines, and formulating assessment reports. Personal information and important data shall not be provided overseas if the result of the security assessment is high or extremely high. The assessment report shall be kept for at least five years. If the data export plan does not satisfy the requirements of lawfulness, appropriateness or controllability, network operators may revise the data export plan or take relevant measures to reduce the risk for data exports (such as desensitization of the data), and initiate another self-assessment.

IV. Focus of Assessment

The self-assessment for data export mainly focuses on two issues, the lawfulness and appropriateness of the export and the controllability of the export.

When assessing the lawfulness and appropriateness of the data export, factors shall be taken into account include whether consent has been obtained from those people whose personal information is to be exported, whether the data export complies with provisions under relevant treaties executed between the Chinese government and other countries or regions, and whether the data export is necessary for performing the ordinary business activities or the contractual obligations of the network operators, and whether the data export is required for judicial assistance.

When assessing the risk controllability of data export plans, features of the exported data and possibility of security incidents during the data export shall be taken into account comprehensively. Features of the exported data include the volume, scope, type, sensitivity and technical process of the personal information or important data. Factors such as (1) technical and management abilities of the exporter in relation to the data export; (2) security protection abilities and measures of the recipient; and (3) the political and legal environment of the jurisdiction of the recipient shall be taken into account when assessing the possibility of security incidents during the data export.

V. Assessment Methods

The Guideline provides methods and standards for assessments, which are based on the levels of impact on personal rights and interests caused by the export of the personal information, the impact on national security and social public interests caused by the export of important data and the degree of possibility of security incidents. On the basis of a comprehensive judgement of the abovementioned factors, the overall security risks of data export activities are classified into four levels, namely extremely high, high, middle and low. After the assessment, if the security

risk of the data export is extremely high or high, the relevant personal information or important data shall not be exported.

VI. Identification of Important Data

The Guidelines defines important data in 28 industries and sectors, such as resources and energy, telecommunications and electronic manufacturing industry, and the definition, scope or identifying criteria for important data in these key industries may be further specified by the competent industry regulators or regulatory authorities. The provisions regarding important data under the Guidelines reflect restrictions on data exports in existing laws and regulations (such as demographic health information, personal financial information, credit information, map information), and adds new types of data restricted from being exported, such as registration information of e-commerce platforms and transaction records of e-commerce.

VII. Observations

As an important ancillary document to the CSL, the Guidelines put forward detailed recommendations on the assessment process, assessment methods and points of the data exports security assessment. Although the Guidelines do not have mandatory legal force, they may be adopted and referred to in data export activities by network operators in various industries since existing laws and regulations fail to provide detailed guidance. In data export assessments, enterprises need to comprehensively take into account factors such as the consent of the individuals whose personal data is being exported, the necessity for data export, the security protection measures of the data exporters and of the data recipient, and the political and legal environment of the receiving country or region. These comprehensive and detailed assessment requirements bring new challenges for enterprises' data export activities. Once assessments determine data export is not allowed, the company may need to consider adjusting its data export practices, improving security protection measures of the data exporter and the data recipient, and taking technical measures such as desensitization to meet compliance requirements. As the Guidelines are still open for public comments, we will continue to monitor its subsequent developments and implementation.

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 6 月 2 日

电信与互联网法律热点问题

数据出境评估指南征求意见

全国信息安全标准化技术委员会（以下简称“**信标委**”）于 2017 年 5 月 27 日公布了《信息安全技术数据出境安全评估指南（征求意见稿）》（以下简称“**《指南》**”），并进行为期一个月的公开征求意见。

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“**《评估办法》**”）。《评估办法》是《中华人民共和国网络安全法》（以下简称“**《网络安全法》**”）重要的配套实施办法，提出了数据安全评估的基本制度框架。根据《评估办法》，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，应当进行安全评估。数据出境安全评估包括自行评估及监管机构评估。《指南》在《评估办法》的基础上，对安全评估的流程、评估要点、评估方法等做出了进一步细化的规定，并界定了各行业和领域“重要数据”的范围和类型。

二、适用范围

《指南》适用于网络运营者开展的个人信息和重要数据出境安全评估工作，也适用于行业主管或监管部门对网络运营者开展个人信息和重要数据出境安全评估进行的指导、监督等工作。网信部门、行业主管或监管部门依职权开展数据出境安全评估亦可参照《指南》执行。

三、安全评估流程

根据《指南》，安全评估流程包括自评估启动、制定数据出境计划、评估数据出境计划的合法正当和风险可控、完成评估报告、检查修正等步骤。

产品或服务涉及向境外提供数据的网络运营者应制定数据出境计划，计划的内容包括但不限于：（1）数据出境目的、范围、类型、规模；（2）涉及的信息系统；（3）中转国家和地区（如存在）；（4）数据接收方及其所在的国家或地区的基本情况；（5）安全控制措施等。

网络运营者应参照《指南》附录 B 的评估方法评估数据出境计划是否合法正当和安全可控，并形成评估报告。如经评估出境安全风险为极高或高的，个人信息和重要数据不得出境。评估报告应至少保存 5 年。如数据出境计划不满足合法、正当要求，或经评估后不满足风险可控的要求，网络运营者可修正数据出境计划，或采用相关措施降低数据出境风险（如数据脱敏），并重新开展自评估。

四、评估要点

数据出境自行评估主要包括合法正当和安全可控两个评估要点。

评估数据出境的合法性、正当性所考虑的因素包括个人信息主体是否已经授权同意个人信息出境；数据出境是否符合我国政府与其他国家、地区签署的相关条约的约定；数据出境是否为网络运营

者在合法的经营范围内从事正常业务活动或履行合同义务所必需；数据出境是否为司法协助需要等。

评估数据出境计划的风险可控，应综合考虑出境数据的属性和数据出境发生安全事件的可能性。出境数据的属性包括个人信息或重要数据的数量、范围、类型、敏感程度和技术处理情况等。对数据出境发生安全事件的可能性的评估要点包括：（1）发送方数据出境的技术和管理能力；（2） 数据接收方的安全保护能力、采取的措施；（3） 数据接收方所在国家或区域的政治法律环境。

五、评估方法

《指南》从个人信息出境对个人权益产生的影响等级、重要数据出境对国家安全及社会公共利益产生的影响等级，以及安全事件的可能性等级等方面规定了相关评估方法及标准。根据对上述内容的综合评价，数据出境活动整体的安全风险分为极高、高、中、低四个等级。经评估，出境安全风险为极高或高的，个人信息和重要数据不得出境。

六、重要数据的识别

《指南》对包括石油天然气、煤炭、石化、电力、通信、电子信息等 28 个行业和领域的重要数据进行了界定，并留待行业主管部门参照《指南》对本行业或领域的重要数据的定义、范围或判定依据作出规范。《指南》所规定的重要数据体现了现有法规中对某些类型的数据出境的限制（如人口健康信息、个人金融信息、征信信息、地图信息等），并在此基础上增加了新的限制出境的数据，如电子商务平台的注册信息和电子商务交易记录等。

七、简评

《指南》是《网络安全法》的重要配套标准，对数据出境评估的流程、方法和要点提出了具体建议。《指南》虽然不具有强制性法律效力，但由于相关法律法规缺乏细节指导规范，《指南》将可能被各行业网络运营者在进行数据跨境传输时所采用和参考。企业需要综合考虑个人数据主体同意、数据出境必要性、数据提供方和接收方安全保障措施、数据接收方所在国家/地区政治法律环境等多方面因素对数据出境进行评估。这些全面、细致的评估要求对企业的跨境数据活动带来了新的挑战。一旦经评估发现存在数据不得出境的情况，企业可能需要考虑采取调整其数据跨境传输实践、完善数据提供方和接收方的安全保障措施、对数据进行脱敏等技术处理等方式以满足合规要求。目前《指南》仍处于征求意见阶段，我们将密切关注《指南》的后续发展及实施情况。

董　潇　　合伙人　电话：86 10 8519 1718　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