JUNHE BULLETIN

July 15, 2022

Data Protection and Cybersecurity

CAC Issues New Measures to Clarify Security Assessment Requirements for Cross-border Data Transfer

I. Introduction

On July 7, 2022 the Cyberspace Administration of China (CAC) issued the *Measures for Security Assessment of Data Export Security* (**Measures**). These Measures will go into effect on September 1, 2022.

On June 30, 2022 CAC released the *Provisions on Standard Contracts for the Export of Personal Information* to seek comments from the public. On June 24, 2022, the National Information Security Standardization Technical Committee of China (TC260) issued the *Specification for the Security Certification of Cross-Border Processing of Personal Information,* which provide guidelines in order to implement the certification mechanism under Article 38 of the *Personal Information Protection Law (the PIPL)*.

The Measures specify the circumstances when the cross-border transfer of personal information is subject to a security assessment. Transfers that are out of the scope of the application can still be justified on a legal basis by way of obtaining a personal information protection certification or entering into a standard contract.

II. Interpretation of the Key Points

The CAC issued a draft of the Measures for public consultation in October last year (**Draft**). The final version remains mostly unchanged from the draft, but some adjustments have been made regarding the scope, conditions and procedures of the security assessments. They aim to provide clearer and more specific guidance for data processors to apply for security assessments, and for the competent authorities to accept and conduct assessments.

This article intends to summarize and comment on the key points of the Measures.

1. Application scope

According to the Measures, if a data processor triggers any of the following thresholds, it needs to apply for a security assessment of its cross-border data transfer: (a) it provides important data abroad; (b) it is a critical information infrastructure operator or it processes the personal information of more than one million individuals in total; (c) it has exported the personal information of more than 100,000 persons in aggregate or the sensitive personal information of more than 10,000 persons in aggregate since January 1 of the previous year; or (d) other circumstances subject to a security assessment as required by the CAC.

2. Specific procedures for a security assessment

If a data export activity triggers a security assessment, the following procedures should be followed:

(a) Pre-review: The data processor should carry out a self-assessment of the risks involved in the data export.

(b) Applying for a security assessment: The data processor should apply to the CAC for a security assessment via the provincial-level cyberspace authority, by submitting: (i) an application form; (ii) a report on the self-assessment; (iii) the legal document to be executed between the data processor and the overseas recipient; and (iv) other materials as required for the security assessment. The provincial-level cyberspace authority is responsible for the complete check of the application materials, and transfer such materials to the CAC.

(c) Carrying out a security assessment: Upon acceptance of the application, the CAC will, depending on the case, organize the relevant departments of the State Council, provincial-level cyberspace authority and specialized institutions to conduct the security assessment. The data processor will be notified in writing of the assessment result.

(d) Re-assessment and termination of a data export: If the validity period of the assessment result has expired or certain circumstances of the re-assessment have occurred during the validity term, the data processor should re-apply for a security assessment. If any data export activity which has already passed the security assessment no longer meets the security requirements for outbound data transfers, such activity should be terminated upon written notice from the CAC.

3. Focused areas for self-assessment and security assessment

The focused areas of self-assessment and security assessment are similar, mainly covering the following six aspects and other matters to be assessed as deemed by the CAC:

(a) the legality, legitimacy, and necessity of the cross-border data transfer in terms of the

purpose, scope, method, etc.;

(b) the impact of data security protection policies and legislation and the cybersecurity environment of the country or region where the overseas recipient is located on the security of the outbound data; whether the data protection level of the overseas recipient meets the requirements of the laws and administrative regulations and the mandatory national standards of the People's Republic of China;

(c) the quantity, scope, type, and sensitivity of the outbound data, and the risks of the data being tampered with, damaged, leaked, lost, relocated or illegally acquired or used during and after the cross-border data transfer;

(d) whether data security and personal information rights and interests can be sufficiently and effectively ensured;

(e) whether the data security protection responsibilities and obligations are sufficiently stipulated in the Legal Document executed between the data processor and the overseas recipient; and

(f) compliance with China's laws, administrative regulations and departmental rules.

4. Legal document to be signed by both parties

The legal document to be executed between the data processor and the overseas recipient should be submitted to the cyberspace authority for a security assessment application. The Measures further require that the data security protection responsibilities and obligations be clearly stipulated in the legal document, and set out specific items that should be contained. This includes the purpose and method of the outbound data transfer and the scope of the data, the purpose and method of the data processing by the overseas recipient, and the measures to handle the data transferred overseas upon the expiration of the retention period, the completion of the agreed purpose, or the termination of the legal document.

In terms of content, the legal document under the Measures is not completely consistent with the standard contract (draft). In terms of formality, the legal document may also include other legally binding documents in addition to contracts. The specific requirements for the contract content will remain to be further explained and confirmed by the CAC.

5. Timelines for security assessments

The CAC should, within seven working days of the date of receipt of the application materials from the local cyberspace authority, determine whether to accept the application, and complete the security assessment within 45 working days of the date of the written notification of acceptance. If the case is complicated or there are materials that need to

be supplemented or corrected, this period may be extended as appropriate and the data processor should be notified of the extension.

6. Circumstances for reapplying for a security assessment

Passing a security assessment for a data export is valid for two years. The circumstances for reapplying for a security assessment under the Measures include: (a) If the data processor needs to continue the data export activity after the expiration of the validity period, it should reapply for the assessment within 60 working days of the expiration date; (b) any circumstance that may affect the security of the outbound data occurs during the validity term, such as a change to the purpose, method, or scope of the data export; (c) In the case whereby the CAC requires a data processor to terminate the data export and the data processor has a need to continue the data export, it should reapply for a security assessment after completing the rectification.

III. Impact and Observation

The Measures clarify the scope, conditions and procedures for a security assessment on data exports, and provides specific compliance guidance for enterprises to carry out data export activities. The Measures provide a six-month transition period from its effectiveness for the rectification of cross-border data transfers carried out before the Measures take effect (September 1, 2022). We suggest enterprises and institutions in various industries take the following measures in a timely manner to meet the corresponding compliance requirements:

- Sort out the data export scenarios of the enterprise, and evaluate the scale and attributes of the data involved;
- Specify priorities and create a timetable for compliance rectification according to importance and sensitivity, and adhere to the timetable;
- Specify the path for the data export and select the appropriate data exporter and overseas recipient according to the data export activities in the different business scenarios and take into consideration the risks and costs involved;
- Establish an internal assessment system, integrate a personal information protection impact assessment and a data export risk self-assessment, and use assessment tools to produce assessment reports that meet the regulatory requirements;
- Further consider security assessment requirements based on a self-assessment; for activities that are subject to an application for a security assessment, conduct effective communication with the regulator in a timely manner;
- Revise and update the legal documents for data export in accordance with the relevant regulations and standard contracts;
- Communicate with overseas recipients of

data in a timely manner, adjust data processing and transmission plans if necessary, and jointly promote compliance with all data export requirements;

- Understand and investigate the legislation and the cybersecurity environment of the country or region where the overseas recipient is located, and keep an eye on any macro risks and legal obstacles;
- Make adjustments as soon as possible for any situation that may fail to pass an assessment based on the self-assessment result, to reduce the impact on the business as much as possible; and
- Constantly follow up on changes relating to the regulatory requirements and practices.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email: dongx@junhe.com
Chao GUO	Associate	Tel: 86 10 8553 7733	Email: guoch@junhe.com

君合研究简讯

2022 年 7 月 15 日

数据安全法律热点问题

国家网信办发布《数据出境安全评估办法》

一、前言

《数据出境安全评估办法》（以下简称“《评估办法》”）由国家互联网信息办公室（“**国家网信办**”）于2022年7月7日审议通过并发布，并将于2022年9月1日起生效实施。

值得注意的是，国家网信办刚于6月30日发布《个人信息出境标准合同规定（征求意见稿）》并向社会征求意见，而全国信息安全标准化技术委员会也于6月24日发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》，以落实《个人信息保护法》第38条规定的认证机制。

从规范个人信息出境活动的角度看，安全评估与前述标准合同和认证的适用相衔接并互为补充。《评估办法》进一步明确了适用安全评估的个人信息出境情形，《评估办法》适用范围外的个人信息处理者的数据出境情形，则可以通过个人信息保护认证或者签订国家网信办制定的标准合同来满足出境条件。

二、重点内容解读

国家网信办曾于去年10月发布《数据出境安全评估办法（征求意见稿）》（“**征求意见稿**”）。与征求意见稿相比，《评估办法》的体例和结构并未有重大变化，但在安全评估的范围、条件和程序上做了若干调整，为数据处理者申报安全评估、主管部门受理和开展评估提供了更为明确和具体的指导。

本文将对《评估办法》的重点内容进行总结和解读。

1. 适用范围

《评估办法》规定数据处理者向境外提供数据有下列情形之一的，应当申报安全评估：（一）向境外提供重要数据；（二）关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；（三）自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息；（四）国家网信办规定的其他情形。

2. 安全评估的具体流程

数据出境活动如符合申报安全评估情形的需遵守下列流程：

(一) 事前评估：数据处理者应开展数据出境风险自评估。

(二) 申报评估：数据处理者应通过所在地省级网信部门向国家网信办申报安全评估，提交材料包括：（1）申报书；（2）数据出境风险自评估报告；（3）数据处理者与境外接收方拟订立的法律文件；（4）安全评估工作需要的其他材料。省级网信部门负责对申报材料完成完备性查验，并将申报材料报送国家网信办。

(三) 开展评估：国家网信办受理申报后，根据申报

情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。评估结果将会书面通知数据处理者。

(四) 重新评估和终止出境：评估结果有效期届满或者在有效期内出现重新评估情形的，数据处理者应当重新申报评估。已经通过评估的数据出境活动不再符合数据出境安全管理要求的，经国家网信办书面通知后应终止。

3. 自评估和安全评估的重点评估事项

自评估和安全评估的评估重点比较类似，主要集中在以下六大方面以及其他网信办认为需要评估的方面。

(一) 数据出境的目的、范围、方式等的合法性、正当性、必要性；

(二) 境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

(三) 出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

(四) 数据安全和个人信息权益是否能够得到充分有效保障；

(五) 数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；以及

(六) 遵守中国法律、行政法规、部门规章情况。

4. 双方签署的法律文件

数据处理者与境外接收方拟订立的法律文件应作为申报材料之一，在申报安全评估时提交至网信部门。《评估办法》进一步要求法律文件应明确约定数据安全保护责任义务，并列举了所需包含的内容，例如数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等，以及数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施。

从内容上看，《评估办法》规定的法律文件与标准合同（草案）并不完全一致，而在形式上，法律文件可能还包括除合同形式之外的其他具有法律效力的文件。对于合同内容的具体要求有待于国家网信办在实践中的进一步解释和确认。

5. 安全评估期限

国家网信办自收到省级网信部门递交的申报材料之日起7个工作日内确定是否受理评估，并自出具书面受理通知书之日起45个工作日内完成安全评估。情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。

6. 重新申报评估的情形

通过数据出境安全评估的结果有效期为2年。根据《评估办法》，重新申报评估的情形包括：（1）有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满60个工作日前重新申报评估；（2）有效期内，发生影响出境数据安全的情形的（如境外接收方处理数据的用途、方式、范围发生变化）；（3）在国家网信办要求数据处理者终止数据出境活动的情况下，如需要继续开展数据出境活动的，数据处理者应在整改完成后重新申报评估。

三、影响和建议

《评估办法》明确了数据出境安全评估的范围、条件和程序，为企业开展数据出境活动提供了具体的合规指引。根据《评估办法》，对于本办法生效（2022年9月1日）前已经开展的数据出境活动，数据处理者应当在生效之日起6个月内完成整改。我们建议各行业的企业和机构应及时采取下述措施以满足相应的合规要求：

- 整体梳理企业的数据出境场景，判断所涉数据的规模和属性；
- 根据重要性和敏感程度，明确合规整改的优先事项和时间表，把握合规时间安排；
- 根据业务场景下的数据出境情况，综合风险和

成本，明确数据出境路径，选择合适的出境方和境外接收方；

- 建立内部评估制度，整合个人信息保护影响评估和数据出境风险自评估，运用评估工具，输出符合监管要求的评估报告；
- 申报安全评估的，可以在自评估的基础上进一步考虑安全评估要求，及时与监管沟通具体要求；
- 参照相关规定和标准合同文本，修改完善数据出境的法律文件；
- 及时与境外接收方开展进行沟通，有必要的对数据处理和传输方案进行调整，共同推进数据出境的合规工作；
- 对境外接收方所在国家和地区的法律政策环境及网络安全环境进行了解和调研，把握宏观风险和法律障碍；
- 根据评估情况，对于根据自评估可能存在评估未能通过的情况，应尽快进行相应的调整，以尽可能地减少对业务的影响；以及
- 持续跟进政策要求和实践变化。

董潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
郭超　律　师　电话：86 10 8553 7733　邮箱地址：guoch@junhe.com