JUNHE BULLETIN

September 5, 2022

Data Export Law

Data Export Compliance Series (III):Official Release of the Application Guidelines for Security Assessment of Data Export (Version 1)

On August 31, 2022, the Cyberspace Administration of China ("**CAC**") officially released the *Application Guidelines for Security Assessment of Data Export (Version 1)* (the "**Application Guidelines**")[1] before the *Security Assessment Measures for Data Export* (the "**Assessment Measures**") officially come into effect. The Application Guidelines specifically address the application scope, methods, procedures, materials, and queries with respect to security assessments of data exports, to provide guidance for data processors who intend to apply for security assessments of data exports.

The local equivalents of CAC have also been making preparations for the application for security assessments of data exports. For example, on September 2, 2022, the Cyberspace Administration of Jiangsu Province released the *Application Guidelines for Security Assessment of Data Export of Jiangsu Province (Version 1)*[2] and the Beijing Municipal Cyberspace Administration now provides an inquiry hotline for further information regarding the Application Guidelines[3].

We have analyzed the more specific processes and requirements stipulated by the Application Guidelines for your reference.

I. Circumstances that Trigger a Security Assessment

The circumstances that trigger an application for a security assessment of data export under the Application Guidelines are consistent with Article 4 of the Assessment Measures. This includes the export of important data, the export of personal information by critical information infrastructure operators and by data processors processing a large amount of personal information, and the export of a large amount of personal information or sensitive personal information. However, no further explanation is provided for the time being on how to calculate each specific threshold that triggers a security assessment, and it remains to be determined on a case-by-case basis and communicated with regulators.

[1] Please refer to the *Application Guidelines for Security Assessment of Data Export (Version 1)* released by the CAC at http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm

[2] Please refer to the *Easy-to-Understand Diagram: Recent Release of Jiangsu Provincial Application Guidelines for Security Assessment of Data Export* at http://www.jswx.gov.cn/xinxi/shuzi/202209/t20220902_3068388.shtml

[3] Please refer to Beijing Municipal *Cyberspace Administration Provides an Inquiry Hotline for Security Assessment of Data Export* at https://mp.weixin.qq.com/s/qt3X4O35a7fFfKbaHDO6Fw

We note that the *Jiangsu Provincial Application Guidelines for Security Assessment of Data Export (Version 1)* provides more specific details regarding important data. It requires data processors to determine whether the exported data constitutes important data by referring to industrial standards or, in the absence of industrial standards, the rules set forth in Article 73 of the *Network Data Security Regulations (Draft for Comments)*[4] regarding the determination of important data, in addition to the definition of "important data" stipulated in the Assessment Measures and it also provides examples of important data.

II. Interpretation of Data Exports

The Application Guidelines also provide more specific rules for the determination of data exports. As mentioned by CAC on July 7, 2022 when answering questions from reporters on issues related to the Assessment Measures, data exports referred to in the Assessment Measures include the following situations: (i) a data processor transmits and stores outside the PRC the data that is collected and generated in its operation within the PRC; and (ii) the data collected and generated by a data processor is stored in the PRC and is available to overseas institutions, organizations or individuals to access or download.[5] The Application Guidelines have revised "access or download" to "query, access, download and output", further clarifying the rules for the determination of data export. The Application Guidelines still retain the expression "other data exports described by CAC," which allows the regulator to interpret more complicated data exports in future regulatory practice. The Application Guidelines do not clarify whether the processing of the personal information of an individual who is located in China by a data processor who is located outside of China pursuant to Paragraph 2 of Article 3 of the *Personal Information Protection Law* constitutes a "data export" requiring security assessment, which is subject to further interpretation by CAC in subsequent regulatory processes.

III. Application Methods and Procedures

There is a requirement under the Assessment Measures that the provincial cyberspace administration shall complete its review of the completeness of the application materials and, if the application materials are determined complete, the provincial cyberspace administration will forward the application materials to CAC. This is described in the flow chart below.

Compared to the application method and procedures under the Assessment Measures, the Application Guidelines provide more specific rules in the following areas:

[4] The Network Data Security Administration Regulations (Draft for Comments) were released by CAC on December 14, 2021.
[5] Please refer to Press Conference of Security Assessment Measures for Data Export at https://mp.weixin.qq.com/s/I_8CoXlwvIAv4vdWQLANZw

1. The application shall be filed with the written application materials and accompanied with electronic copies thereof (in the form of a CD-ROM);

2. If the application materials are determined incomplete by the provincial cyberspace administration, the data processor will be given a notice of return of the application and will have no further avenue for any addition or correction at this stage;

3. The data processor shall complete a self-assessment three months prior to the date of the application, and no material change will have occurred to it as of the date of the application; and

4. CAC and the local equivalents of CAC will provide telephone numbers and email addresses for inquiries regarding security assessment of data export.

IV. Application Materials and Highlights

Compared to the Assessment Measures, the most significant change reflected in the Application Guidelines is the imposition and enforcement of more specific requirements on application materials for security assessment of data export and the provision of relevant templates.

1. The more specific application materials include:

   (1) A Unified Social Credit Code Certificate;

   (2) An identity document of the legal representative;

   (3) An identity document of the authorized representative for filing the application;

   (4) The power of attorney for the authorized representative for filing the application (template);

   (5) The Application Form for Security Assessment of Data Export (template), including the Letter of Undertaking and the Application Form for Security Assessment of Data Export;

   (6) The contract or other legally binding document to be executed by the data processor and the overseas recipient with respect to the data export;

   (7) The Risk Self-Assessment Report on Data Export (template); and

   (8) Any other supporting material.

2. The above application materials reflect the following updates:

   (1) The Letter of Undertaking requires data processors to provide undertakings not only on the lawful collection and use of exported data, but also on the authenticity, accuracy, completeness and validity of the application materials;

   (2) The Application Form for Security Assessment of Data Export requires data processors to provide particulars of its own and of the data export, the data to be exported, the overseas recipient, and legal documents for the data export. It is especially noteworthy that

   - data processors are required to provide particulars of data security officers and management bodies of its own and the overseas recipient;
   - if the data to be exported includes both personal information and important data, data processors are required to

provide particulars of both;

- data processors are required to describe the scale (MB/GB/TB) of the data, in addition to the category of the data to be exported;
- data processors are required to describe the data export link, such as the link provider, quantity and bandwidth of the links, the name of the data center and the physical location of the server room within and outside of China, and the IP address
- with respect to the clauses required to be contained in the export-related legal documents in accordance with Article 9 of the Assessment Measures, data processors are required to specify the name of the document, the relevant clauses, and the pages containing such clauses, in each legal document; and
- data processors are also required to describe the administrative penalties, investigations, and rectifications imposed by the competent regulatory authorities on it during its business operations in the last two years, with an emphasis on those related to data security and cybersecurity.

(3) CAC provides a Risk Self-Assessment Report on Data Export (Template) to give specific guidance for data processors in preparing their self-assessment reports. We summarize below the specific highlights of this template.

V. Highlights of Risk Self-Assessment Report on Data Export (Template)

The Application Guidelines also provide a Risk Self-Assessment Report on Data Export (Template) ("**Self-Assessment Report Template**"), which sets forth the specific matters to be assessed and analyzed in the self-assessment report and provides important guidance and reference for data processors in preparing the self-assessment report.

1. The self-assessment is required to be completed three months prior to the application for security assessment of data export, and no material change shall occur as of the date of application;
2. In the case of any third-party institution participating in the self-assessment, the data processor is required to describe the basic particulars of the third-party institution, and the participation of the third party in its assessment and affix the official seal of the third-party institution to the pages containing the description;
3. The self-assessment report shall include four parts: a brief description of the organization and implementation of the self-assessment, an overview of the data export, a risk assessment of the proposed data export, and a conclusion of the risk self-assessment of the data export. It is noteworthy that data processors in the self-assessment report are required to address:

   (1) The particulars of the data processor, not only the general registered information and the business and information system involved in the data export, but also the actual controller, general business and data, and investments in or outside of China;

   (2) An assessment of the data security protection capability of the data processor. This includes the establishment of a governance structure and management rules, the

management plan for the entire process, classification and rating, emergency response, risk assessment, protection of personal information rights and interests, and other rules and policies, and the implementation of the foregoing. It also should include the technical security measures adopted through the entire process of the data collection, storage, use, processing, transmission, provision, disclosure and deletion as well as proof of the effectiveness of the data security protection measures, such as the data security risk assessment, the data security capability certification, and the classified cybersecurity protection assessment (MLPS);

(3) An assessment of the overseas recipient, not only describing the particulars of the overseas recipient, the data security protection capacity of the overseas recipient, and the data security protection rules and regulations and cybersecurity environment in the country or region where the overseas recipient is located, but also describing the entire flow chart of data processing by the overseas recipient;

(4) A risk assessment of each of the significant matters required to be assessed under Article 5 of the Assessment Measures, with an emphasis on the issues and potential risks identified by the assessment, and the corresponding corrective measures taken and their effectiveness; and

(5) The conclusion of the risk self-assessment, with full reasons and arguments to support such a conclusion.

VI. Our Observations and Suggestions

The above is our summary of the specific rules and additional requirements under the Application Guidelines with respect to security assessment of data export. We hereby provide the following preliminary advice for enterprises on how to comply with such rules and requirements:

1. If you have not yet reviewed your data exports, it is advised to start checking and reviewing them as soon as possible to determine whether they are subject to application for security assessment of data export in accordance with the Assessment Measures. Considering the overall compliance arrangements, it is advised to complete preparation work as soon as possible.

2. If you do need to apply for security assessment of data export,

   (1) It is difficult to complete applications with both CAC and the provincial equivalent of CAC, and successfully pass their security assessment of data export within the six-month remedy period required under the Assessment Measures, therefore it is advised to engage a third-party professional institution to help you make a project plan using backward scheduling method and specify the responsibilities and obligations of all participants in a security assessment of data export, so as to complete the preparation and submission of the application materials as soon as possible;

   (2) It is advised to conduct a self-assessment on data export to assess each matter required to be assessed in the self-assessment report template and make every effort to correct and rectify issues and problems identified in self-assessment; and

(3) It is advised to prepare other application materials concurrently as required by the Application Guidelines.

3. It is also advised to consider deployment of localization system in advance according to your own specific situation, to avoid any impact on business continuity in the case of your failure to pass the security assessment of data export.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email: dongx@junhe.com
Yang LIU	Partner	Tel: 86 10 8519 1261	Email: liuyang@junhe.com
Shuoying LI	Associate	Tel: 86 21 2208 6242	Email: lishuoying@junhe.com

君合研究简讯

JUNHE

2022 年 9 月 5 日

数据出境法律热点问题

数据出境合规系列三：《数据出境安全评估申报指南（第一版）》正式发布

在《数据出境安全评估办法》（以下简称“**《评估办法》**”）正式生效前夕，国家互联网信息办公室（以下简称“**国家网信办**”）于 2022 年 8 月 31 日正式发布了《数据出境安全评估申报指南（第一版）》（以下简称“**《申报指南》**”）[1]，针对数据出境安全评估的适用范围、申报方式及流程、申报材料、申报咨询等内容作出了具体说明，为拟申报数据出境安全评估的数据处理者提供指导。

同时，我们也注意到，各地网信办也陆续就安全评估的申请开始推进相应的筹备工作，例如，江苏省互联网信息办公室在 2022 年 9 月 2 日发布了《江苏省数据出境安全评估申报工作指引（第一版）》[2]，北京市互联网信息办公室也设立了数据出境安全评估申报咨询电话[3]。

以下是我们对《申报指南》主要细化的流程和要求的分析和解读。

一、触发安全评估的范围

《申报指南》对数据出境安全评估申报范围的规定与《评估办法》第四条保持了严格一致，即包括了重要数据出境、关键信息基础设施运营者和处理大量个人信息的数据处理者个人信息出境，以及大量个人信息或敏感个人信息出境的几种情形，而暂未就实操之中涉及的每一条数据出境安全评估的具体触发条件的计算方式提供进一步的解释和说明。该等计算仍需根据项目的具体情况进行判断、并与主管部门进行沟通。

我们也注意到，《江苏省数据出境安全评估申报工作指引（第一版）》中对重要数据的范围进行了一定的细化和说明，即在《评估办法》所规定的“重要数据”定义基础上，数据处理者需要根据行业标准确定出境数据是否构成重要数据；如无行业标准，可参考《网络数据安全管理条例（征求意见稿）》[4]第七十三条所列举的重要数据的判断标准，并对于重要数据进行了相应的例举。

二、数据出境情形的解释

《申报指南》对数据出境行为的认定进行了细化。国家网信办于 2022 年 7 月 7 日就《评估办法》相关问题回答记者提问时曾提到，《评估办法》所称数据出境活动主要包括：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外。二是数据处理者收集和产生的数据存储在境内，境外

[1] 国家互联网信息办公室发布《数据出境安全评估申报指南（第一版）》，http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm

[2] 《一图读懂|江苏省数据出境安全评估申报工作指引来了》，http://www.jswx.gov.cn/xinxi/shuzi/202209/t20220902_3068388.shtml

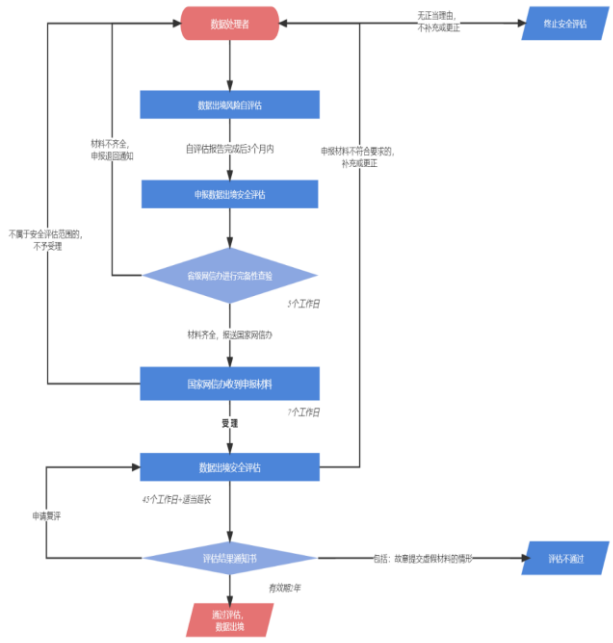
[3] 《北京市网信办开通数据出境安全评估申报咨询电话》，https://mp.weixin.qq.com/s/qt3X4035a7fFfKbaHDO6Fw

[4] 国家网信办于 2021 年 11 月 14 日发布《网络数据安全管理条例（征求意见稿）》

的机构、组织或者个人可以访问或者调用[5]。《申报指南》将“访问或者调用”细化为“查询、调取、下载、导出”，进一步明确了对于数据出境行为的判断标准。《申报指南》保留了“国家网信办规定的其他数据出境行为”的表述，为以后监管实践中可能较为复杂的数据出境情况预留了解释空间。另外，《申报指南》并未明确符合《个人信息保护法》第三条第二款所规定的在境外处理境内自然人个人信息的活动是否属于需进行安全评估的“数据出境”情形，仍需待国家网信办在后续监管过程之中的进一步解释。

三、申报方式及流程

《评估办法》规定数据出境安全评估应首先由省级网信办对申报材料进行完备性查验，申报材料齐全的，申报材料将报送至国家网信办。具体流程请参见下图。



相较于《评估办法》所规定的申报方式和流程，《申报指南》在以下方面进行了细化：

1. 申报方式均为送达书面申报材料并附带材料电子版（光盘方式）；
2. 如果申报材料未通过省级网信办的完备性核验，数据处理者将收到申报退回通知，而没有在此阶段进行补充或更正的机会；
3. 数据处理者就数据出境进行的自评估应在申报之日前 3 个月内完成，且至申报之日未发生重大变化；
4. 国家网信办和部分地方网信办已公布了申报咨询电话和邮箱，方便企业就数据出境安全评估中的问题进行事先咨询。

四、申报材料及相关要点

与《评估办法》相比，《申报指南》本次最主要的变化是细化和落实了数据出境安全评估申报材料的具体要求，并提供了相应的模板。

1. 细化的申请材料包括：
   (1) 统一社会信用代码证件；
   (2) 法定代表人身份证件；
   (3) 经办人身份证件；
   (4) 经办人授权委托书（模板）；
   (5) 数据出境安全评估申报书（模板），包含《承诺书》与《数据出境安全评估申报表》两个部分；
   (6) 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件；
   (7) 数据出境风险自评估报告（模板）；以及
   (8) 其他相关证明材料。
2. 针对上述申请文件，主要的更新要点如下：
   (1) 《承诺书》要求数据处理者既要对其

[5] 《<数据出境安全评估办法>答记者问》，https://mp.weixin.qq.com/s/I_8CoXlwvIAv4vdWQLANZw

出境数据的合法收集和使用进行承诺，又要对申报材料的真实、准确、完整和有效进行承诺；

(2) 《数据出境安全评估申报表》要求数据处理者提供与其自身、数据出境业务、拟出境数据、境外接收方以及出境法律文件相关的基本信息，特别需要注意的是：

- 数据处理者需要同时提供其自身以及境外接收方的数据安全责任人和管理机构的情况；
- 拟出境数据同时包括个人信息和重要数据的，需要一并进行申报；
- 除拟出境数据的种类外，数据处理者需要对数据规模（MB/GB/TB）进行描述；
- 数据处理者需对数据出境链路进行描述，包括链路提供商、链路数量与带宽、境内外落地数据中心名称及机房物理位置、IP 地址等；
- 《评估办法》第九条所要求体现的出境法律文件必备内容，应由数据处理者逐一标明对应的文件名、页码和条款；以及
- 数据处理者需简述其在近 2 年内在业务经营活动中受到行政处罚和有关主管监管部门调查及整改的情况，并重点说明数据和网络安全方面的有关情况。

(3) 国家网信办提供了数据出境风险自评估报告（模板），为数据处理者准备自评估报告提供了具体指导。我们将在下文进行具体的重点提示。

五、数据出境风险自评估报告模板之中的要点

针对《申报指南》颁发之前数据处理者普遍关心的数据出境风险自评估报告，《申报指南》本次也提供了《数据出境风险自评估报告》（模板）（以下简称“**自评估报告模板**”），列明了自评估报告所需评估和分析的具体内容，为数据处理者准备自评估报告提供了重要指导和参考：

1. 自评估活动需要在数据出境安全评估申报前 3 个月内完成，且至申报之日未发生重大变化。
2. 如有第三方机构参与自评估，数据处理者须在自评估报告中说明第三方机构的基本情况及参与评估的情况，并在相关内容也上加盖第三方机构公章。
3. 自评估报告包括四大方面：组织和实施自评估的基本情况、出境活动的整体情况、拟出境活动的风险评估情况以及出境活动风险自评估结论。特别提示注意的是：

   (1) 数据处理者的基本情况，不仅限于一般的登记信息以及数据出境涉及的业务和信息系统，还需要披露企业的实际控制人、整体业务和数据情况、境内外投资情况；

   (2) 对数据处理者的数据安全保障能力的评估，既包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况；又包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施；并且还应就其数据安全保障措施有效性提供证明，例如数据安全风险评估、数据安全能力认证、网络安全等级保护测评等；

   (3) 针对境外接收方的评估，除了境外接

收方的基本情况、数据安全保障能力及其所在国家和地区的数据安全保护政策法规和网络安全环境，自评估报告模板还要求描述境外接收方处理数据的全流程过程；

(4) 针对《评估办法》第五条所规定的重点评估事项，自评估报告模板要求逐项说明风险评估情况，重点说明评估发现的问题和风险隐患，以及相应采取的整改措施和整改结果；

(5) 自评估报告的结论应充分说明得出自评估结论的理由和论据。

六、我们的观察和建议

以上我们总结了《申报指南》就数据出境安全评估作出的细化和新增要求，企业在实践中如何落实这些内容，我们初步建议如下：

1. 如果企业尚未对数据出境活动进行梳理，建议尽快启动数据出境活动的核查和梳理，确定是否需要按照《评估办法》申报数据出境安全评估，考虑到整体合规的安排，准备工作需要紧凑的安排完成；

2. 对于确定需要进行数据出境安全评估的企业来说：

(1) 在《评估办法》规定的 6 个月整改期限内完成省级网信办以及国家网信办的两级申报并顺利通过数据出境安全评估，具有一定的难度，建议企业可在第三方专业机构的协助下，倒排项目时间表，落实数据出境安全评估所涉及的各方主体的责任和义务，争取尽早完成申报材料的准备和提交；

(2) 尽快按照自评估报告模板所列举的各项评估内容对出境活动进行自评估，并对自评估过程中发现的问题和差距积极进行整改并落实整改措施；以及

(3) 按照《申报指南》的要求同步准备其他申报材料。

3. 企业也需根据自身具体情况考虑提前进行数据本地化部署，避免在数据出境安全评估未通过的情况下其业务持续运营受到影响。

董潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
刘洋　合伙人　电话：86 10 8519 1261　邮箱地址：liuyang@junhe.com
李硕颖　律师　电话：86 21 2208 6242　邮箱地址：lishuoying@junhe.com