

CHINA REGULATORY UPDATES



瀚一律师事务所
HAN YI LAW OFFICES

www.hanyilaw.com

August - October, 2022



TABLE OF CONTENTS / 本期内容

DATA SECURITY / 数据安全

China Strengthened Measures on Data Export / 中国进一步完善数据出境相关规定

2



DATA SECURITY / 数据安全

China Strengthened Measures on Data Export 中国进一步完善数据出境相关规定

2022年7月7日，国家互联网信息办公室（“网信办”）正式发布《数据出境安全评估办法》（“《评估办法》”），自2022年9月1日起实施。《评估办法》的主要内容与2021年10月发布的征求意见稿（关于征求意见稿的解读，参见我所《每月立法动态》2021年11月刊）基本相同，明确规定了数据出境安全评估的范围、条件和程序，为数据出境安全评估工作提供了具体指引。值得注意的是，针对必须进行出境安全评估的“重要数据”，《评估办法》从影响“国家安全、经济运行、社会稳定、公共健康和安全”的角度作了概括性的定义，但该规定在具体执行时将如何适用仍存在较大不确定性。根据我们了解，目前网信办关于“重要数据”的认定主要参考《网络数据安全条例（征求意见稿）》（主要包括七大类数据；具体分析请参见于2022年3月3日刊发于我所主页的《企业需知的十个网络和数据安全合规事项》）中的相关规定，并视情况咨询相关企业的行业主管部门的意见。此外，《评估办法》还进一步明确了存量数据出境业务的整改期限，要求目前已开展的数据出境活动的企业在6个月内（即2023年3月1日前）按照《评估办法》完成合规整改。

为配合《评估办法》的施行，引导数据处理者规范、有序地申报数据出境安全评估，2022年8月31日，网信办发布《数据出境安全评估申报指南（第一版）》（“《申报指南》”），对数据出境安全评估的申报方式及流程、申报材料等事项作出了细化说明。针对实践中形式多样、层出不穷的数据跨境流动场景，《申报指南》正式明确了受规范的“数据出境”行为包括：(i)将在境内收集和产生的数据传输、存储至境外；(ii)收集和产生的数据存储在国内，境外的机构、组织或者个人可以查询、调取、下载、导出（此点进一步细化了网信办在相关新闻发布会上描述的境外远程访问的场景）；以及(iii)网信办规定的其他数据出境行为。相关数据处理者需要特别注意识别其所涉及的数据流动活动是否可能构成《评估办法》及《申报指南》下的“数据出境”行为。

2022年9月12日，网信办发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》，拟进一步提高危害网络安全、违反安全审查规定等违法行为的法律责任。其中，对于违法行为情节特别严重的相关责任主体，处罚上限大幅提升，最高或将面临“人民币5,000万元”或者“上一年度营业额5%”的罚款。

随着近期数据出境相关规定的不断出台，中国的数据出境监管体系已经基本确立。从合规角度，我们建议相关企业及时按照新要求对数据出境活动进行识别及规范（包括但不限于建立内控制度、修订业务合

On July 7, 2022, the Cyberspace Administration of China (or CAC) formally issued the *Measures on Security Assessment for Data Exports* (the “Measures”) which has become effective as of September 1, 2022. This final version is generally consistent with the draft released in October 2021 (*please refer to our November 2021 issue of China Regulatory Updates for more details*), while setting out some detailed guides on such key aspects as the scope, the application requirements and the procedures of security assessment. Notably, with respect to the scope and definition of “important data”, which is subject to security assessment by CAC before being exported, the Measures only provides a very general principle (i.e., the important data shall be determined based on its influence in terms of national security, economy, social stability, or public health and safety), which may lead to practical uncertainties and confusions. Based on our inquiries with CAC on a no-name basis, when identifying important data, at this initial stage CAC would like to make a general reference to the definition provided under the Draft Regulations on Network Data Security Management (which spelt out a list of typical important data in major industries; *for more details, please refer to our memorandum PRC Data and Cyber Security Compliance - 10 most common questions facing companies operating in China published on March 3, 2022*), and if necessary, to seek advice from the government authorities in charge of the industries concerned. For data processors already engaged in data export activities, the Measures provides a 6-month transitional period for them to take rectification measures to fully comply with the Measures before March 1, 2023.

To better implement the Measures, on August 31, 2022, CAC released the *Guidelines for Application for Security Assessment for Data Exports (First Edition)* (the “Guidelines”), providing more practical guidance on application form, materials and process, among others. In terms of diverse cross-border data flow scenarios in practice, the Guidelines clarifies the definition of “data export” activities as: (i) outbound transmission or storage of data collected or generated domestically; (ii) access to, retrieval, download or export by foreign entities data stored or generated domestically (*which provides more detailed guidance on the remote access scenario as described by CAC in its press conference at the release of the Measures*); or (iii) other outbound data activities stipulated by CAC.

Furthermore, on September 12, 2022, CAC issued the *Decision on Amendments to the PRC Cybersecurity Law (Draft for Comments)*, which proposes to further increase the liabilities of data processors for violation of cybersecurity or security assessment regulations, among others. According to the draft amendments, for severe violation activities, economic penalties are proposed to be increased to a fine of up to RMB50 million or 5% of the violating entity’s total revenue of the previous year.

With the recent issuance and amendments of regulations on data export activities, China has generally established the legislative framework in the regime of data export. For data processors, measures are suggested to be taken to prudently examine and optimize their data processing activities (especially those related to data export or national security) in line with the new regulations to reduce compliance risks (including, but not limited to, improving internal data process SOPs, regularly making internal and external data security assessment, and strengthening data security requirements when dealing with

同、通过安全评估等），以降低相关合规风险。我们将对相关规定的后续修订和实践中的落地情况保持关注。

vendors and business partners). We will continue to monitor and update PRC regulatory as well as practical developments in this area.

These updates are intended for information purpose only and are not a legal advice or a substitute for legal consultation for any particular case or circumstance. © Han Yi Law Offices All Rights Reserved.

For further information, please write us at inquiry@hanyilaw.com.

CONTACT US

上海市中山西路2020号
华宜大厦1座1801室
邮编：200235
电话：(86-21) 6083-9800



Suite 1801, Tower I, Huayi Plaza
2020 West Zhongshan Road
Shanghai 200235, China
Tel: (86-21) 6083-9800