汉坤法律评述
漢坤律師事務所
融贯中西 · 务实创新
2017 年 4 月 13 日

数据出境不再任性

---深度评析《个人信息和重要数据出境安全评估办法(征求意见稿)》

唐志华丨朱敏

2017 年 4 月 11 日，国家网信办发布了《个人信息和重要数据出境安全评估（征求意见稿）》（“《评估办法》”），公开征求意见，以完善即将于 2017 年 6 月 1 日生效的《网络安全法》。作为《网络安全法》的重要配套文件之一，《评估办法》意在具体落实《网络安全法》第三十七条规定的个人信息和重要数据出境安全评估。虽然目前《评估办法》仅是征求意见稿，但从其具体内容看，数据跨境转移的监管重点已一览无遗。

一、 监管对象 - 不管你是什么企业

本次《评估办法》明显扩大了数据出境安全评估义务人的范围。

《网络安全法》第三十七条规定，“关键信息基础设施的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，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估”。同时，《网络安全法》对“关键信息基础设施”的范围在第三十一条也有限定，即“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”。据此，《网络安全法》下的数据存储本土化和出境安全评估义务仅适用于运营关键信息基础设施的企业。

但是，《评估办法》将数据存储本土化和出境安全评估的要求适用于所有网络运营者。根据《评估办法》第二条，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，应当按照本办法进行安全评估。此外，《评估办法》第十六条要求其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。虽然理论上，本条规定对网络运营者之外的企业不具有直接的强制适用效力，但从目前个人信息和重要数据跨境传输的立法趋势和监管态势来看，“被参照”的个人和组织在同等或类似情形中显然是要被新规所覆盖的。

从《评估办法》的上述两条规定，显而易见，凡存在数据跨境传输行为的企业都有可能都被囊括在安全评估的监管范围之内，这无疑将增加企业的合规成本和负担，尤其是从事跨境的企业管理、融资活动、信息服务、数据存储、技术研发、网络平台等行业或活动的企业，将会受安全评估的严格监

管。我们估计该等适用范围的扩大可能会引起市场的强烈反响，也将是征求意见反馈的异议热点。

二、 监管内容 - 不管你是什么数据

《评估办法》第八、九和十一条分别从评估内容、需报请行业主管或监管部门评估的情形和不得出境的数据等方面对不同类型、不同情形的数据跨境传输进行全方位的监管。

1. 数据出境安全评估重点

《评估办法》第八条规定，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) 涉及个人信息情况，包括个人信息的数量、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) 涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；

4) 数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

5) 数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

6) 数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

7) 其他需要评估的重要事项。

对于个人信息出境，《评估办法》要求网络运营者应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。除此之外，《评估办法》第十二条要求，当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。

2. 报请数据出境安全评估

《评估办法》第九条规定，出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：

1) 含有或累计含有 50 万人以上的个人信息；

2) 数据量超过 1000GB；

3) 包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；

4) 包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；

5) 关键信息基础设施运营者向境外提供个人信息和重要数据；

6) 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。

安全评估应当于六十个工作日内完成，并及时反馈网络运营者，上报国家网信部门。行业主管或监管部门不明确的，由国家网信部门组织评估。

3. 不得出境的数据

《评估办法》在第十一条规定了几类不得出境的数据，包括：

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) 其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

《评估办法》的上述规定，从评估的重点、评估的方式，到数据的性质、信息的数量等角度，在扩大评估适用义务人范围的基础上，对跨境数据传输实施了几乎全覆盖的监管。

三、 责任承担 - 企业都得兜着

《评估办法》第六、七、九和十二条规定了出境数据安全评估的具体方式。在数据出境前，企业应以自评为主。一般情况下，企业自行组织对数据出境进行安全评估，对评估结果负责；特殊情形下，包括遇到上文提到的法定情形，企业应报请行业主管或监管部门进行评估，由监管部门决定是否可以出境。

我们认为，这些规定释放了一个很明显的信号，即安全评估相当强调企业的主体责任：对于一般情形（第六条），企业自行评估，并对评估结果负责；对于特定情形（第九条），企业应当主动报请有关部门参与评估。企业显然被放在了一个第一责任人并担负主要评估责任的位置。由此，对企业而言，在一般情形中，如果未开展自行评估，或在自行评估中存在任何隐瞒、欺诈或造假行为，或在特殊情形中，如果未及时报请行业主管或监管部门进行评估而擅自开展数据跨境传输行为，都会面临监管机构的整改要求，甚至处罚。

四、 企业该怎么办？

《评估办法》对《网络安全法》中提及的部分概念性条款作了阐明和注释，无疑对企业数据存储和跨境传输的合规性提供了进一步的指引。但《网络安全法》中部分待明确的概念在《评估办法》中仍未解释清楚，或者《评估办法》本身又引申出了一些待定问题。

例如，“重要数据”，在《评估办法》中，被定义为“与国家安全、经济发展，以及社会公共利益密切相关的数据”，但又将具体范围推给了不知何时出台的国家标准和识别指南。再如，“关键信息基础设施运营者向境外提供个人信息和重要数据必须报请安全评估”，但是对“关键信息基础设施”的具体范围，除了《网络安全法》中的列举描述和目前普遍参考的《国家网络安全检查操作指南》，国务院也仍未正式出台相关文件，《评估办法》也未提及。再如，《评估办法》规定“未经个人信息主体同意”的个人信息不得出境，以何种方式才算有效获得了信息主体的同意？这对信息主体覆盖面相当广的银行金融、医疗健康、互联网以及其他公共服务行业而言显得尤为重要。

随着《网络安全法》正式施行的临近，这些概念的模糊不清将会对企业数据出境操作的合规带来不确定性，也必然增加了企业的合规风险。鉴此，在《网络安全法》正式施行而配套规定尚未完善之际，我们建议企业：

1. 应尽早建立数据存储和跨境传输的内控政策以及出境安全的评估机制；对已建立相应政策

和机制的企业，则应根据《评估办法》的要求进行对照审查，调整修改。同时，结合《评估办法》第八条规定的评估重点内容，内部先行梳理出境数据的性质、数量，从管理、业务、市场、融资等方面入手，准备数据出境的必要性分析。

2. 建设和完善信息保护和数据安全的软硬件设施，了解数据出境目的地的网络安全状况，确保与出境数据的境外接收方形成有效的联动机制。

3. 尤为重要的是，企业在发生跨境数据或信息传输前，与行业主管或监管部门进行有效的沟通，对可能的数据出境行为先行报备，了解清楚出境数据的评估属于自我评估还是报请评估，以大大减少数据传输的合规成本和风险。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤**唐志华律师（+8621-6080 0905; david.tang@hankunlaw.com**）或**朱敏律师（+8621-6080 0955; min.zhu@hankunlaw.com**）联系。