汉坤法律评述
2021 年 10 月 29 日

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

国家网信办《数据出境安全评估办法（征求意见稿）》公开征求意见

作者：段志超 | 蔡克蒙 | 王雨婷[1]

2021 年 10 月 29 日，国家互联网信息办公室（“**网信办**”）发布《数据出境安全评估办法（征求意见稿）》（“**《征求意见稿》**”），向社会公开征求意见。《征求意见稿》旨在细化和落实《网络安全法》第 37 条、《数据安全法》第 31 条、《个人信息保护法》第 36、38、40 条等法律中有关数据出境的规定。相较此前征求意见稿[2]，《征求意见稿》体现了严格管理数据出境的立场：如设置较低的政府评估数量门槛，要求企业坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，以及将安全评估权限上收到国家网信办层面。与之对应的，《征求意见稿》亦规定了严重的违规后果，在数据出境评估结果的二年有效期内出现规定情形但未重新申报评估的，或有效期届满未按规定重新申报评估的相关主体将不得进行数据出境活动。

本文旨在从涉数据出境企业的视角，简析有关本《征求意见稿》揭示的有关数据出境安全评估的注意事项与潜在挑战。

一、广泛的适用范围

《征求意见稿》第 2 条规定，数据处理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重要数据和依法应当进行安全评估的个人信息，应当进行数据出境安全评估。第 4 条进一步明确了需要申报政府评估的五种情形：

- 关键信息基础设施的运营者收集和产生的个人信息和重要数据；（对应《网络安全法》第 37 条）
- 出境数据中包含重要数据；
- 处理个人信息达到一百万人的个人信息处理者向境外提供个人信息；
- 累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息；
- 国家网信部门规定的其他需要申报数据出境安全评估的情形。

[1] 实习生李阳阳对本文的写作亦有贡献。

[2] 网信办于 2017 年发布《个人信息和重要数据出境安全评估办法（征求意见稿）》，信息安全标准化委员会于 2017 年发布的《数据出境安全评估指南（征求意见稿）》，两年后网信办于 2019 年 6 月发布《个人信息出境安全评估办法（征求意见稿）》。

除了重申《网络安全法》第 37 条关键信息基础设施运营者数据出境的安全评估要求，并对重要数据出境予以持续强化监管，本《征求意见稿》最大的亮点系对《个人信息保护法》第 40 条“处理个人信息达到国家网信部门规定数量的个人信息处理者”的标准予以了明确。

实践中，企业常提出的问题是第 40 条的规定数量究竟应按照企业（或企业集团）掌握个人信息的数量，或是相关信息系统处理个人信息的数量，或是特定处理活动中提供个人信息的数量为标准进行统计。对此，《征求意见稿》提出了“处理数量”与“提供数量”两个计算标准。“处理个人信息达到一百万人的个人信息处理者”似以某个特定数据处理者（理论上应以法人主体为单位）涉及的信息主体的总量计算（可能将各类系统中的个人信息加总计算），而“累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息”则似以特定数据处理者在具体提供活动中涉及的信息主体数量为标准计算。这两项数量标准均设置的较低，达到二者之一即需申请政府评估。

前述较低的规定数量的设计将对跨境数据传输实践产生深远的影响。各类提供 2C 产品或服务的跨国公司以及即使提供 2B 产品或服务、不掌握消费者个人数据，但可能在华雇佣大量员工或掌握大量 B 端客户联系人的跨国公司均必需申请政府安全评估方可向境外传输个人信息。相关存在相关数据出境活动的企业均应积极开展自查，一旦处理或累计提供个人信息达到前述量级，或涉及向境外提供重要数据，在《征求意见稿》落地后，可能均需就数据出境活动提交网信部门安全评估。

二、企业自查为先导

《征求意见稿》第 5 条要求在向境外提供数据前，应事先开展数据出境风险自评估，自评估应重点评估以下事项：

- 数据出境及境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；
- 出境数据的数量、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；
- 数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险；
- 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
- 数据出境和再转移后泄露、毁损、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等；
- 与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务。

第 6 条将“数据出境风险自评估报告”与“数据处理者与境外接收方拟订立的合同或者其他具有法律效力的文件等”（以下统称“**合同**”）作为申报数据出境安全评估的重点审查材料之一，后者要求合同应充分约定数据安全保护责任义务。第 9 条指出，合同应包括以下条款：

- 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；
- 数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者合同终止后出境数据的处理措施；
- 限制境外接收方将出境数据再转移给其他组织、个人的约束条款；
- 境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化导

致难以保障数据安全时，应当采取的安全措施；

- 违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款；
- 发生数据泄露等风险时，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。

三、政府评估为核心

在重视以“合同”与“自评估”的形式推动企业自我管控数据出境风险的同时，《征求意见稿》仍强调政府对数据出境的“事先审查”在数据出境安全管理中的核心作用。凡具备第 4 条规定情形的数据处理者，均需在出境前申请政府数据安全评估，数据出境安全评估以网信部门为主管部门。申报评估的流程如下：

- 数据处理者通过所在地省级网信部门向国家网信部门申报数据出境安全评估，并提交申报材料；（第 6 条）
- 国家网信部门自收到申报材料之日起七个工作日内，确定是否受理评估并以书面通知形式反馈受理结果；（第 7 条）
- 国家网信部门受理申报后，组织行业主管部门、国务院有关部门、省级网信部门、专门机构等进行安全评估。涉及重要数据出境的，国家网信部门征求相关行业主管部门意见；（第 10 条）
- 国家网信部门自出具书面受理通知书之日起四十五个工作日内完成数据出境安全评估；情况复杂或者需要补充材料的，可以适当延长，但一般不超过六十个工作日。评估结果以书面形式通知数据处理者。（第 11 条）

第 8 条规定，政府评估应侧重于：

- 数据出境的目的、范围、方式等的合法性、正当性、必要性；
- 境外接收方所在国家或者地区的数据安全保护政策法规及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、行政法规规定和强制性国家标准的要求；
- 出境数据的数量、范围、种类、敏感程度，出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险；
- 数据安全和个人信息权益是否能够得到充分有效保障；
- 数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务；
- 遵守中国法律、行政法规、部门规章情况。

相较 19 年征求意见稿[3]，《征求意见稿》将评估权限上收到国家网信办层面，并要求在重要数据出境安全评估过程中征求行业主管部门意见，而评估期限为材料受理后 45 个工作日，甚至可能延长至 60 个工作日甚至更长。实践中，企业的数据处理活动通常具有时效性和连续性，较长的审查期限可能对企业运营相关

[3] 《个人信息出境安全评估办法（征求意见稿）》第七条 省级网信部门在将个人信息出境安全评估结论通报网络运营者的同时，将个人信息出境安全评估情况报国家网信部门。网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的，可以向国家网信部门提出申诉。

的各类客户数据、员工数据跨境传输带来较大的不确定性。

四、持续评估和监管

数据出境安全评估并非完成一次评估即可一劳永逸，《征求意见稿》旨在建立持续的评估和监管机制。数据处理者在数据出境评估结果的二年有效期内可正常开展数据出境活动。但在有效期内发生了需重新申报评估的情形，或评估结果有效期届满的，则应重新申报评估。

具体而言，数据处理者通过网信办数据出境安全评估后，在二年内无需就同一接收者后续的多次或连续的传输类似数据申请重新评估。然而，在下列情形下（第 12，16 条），数据处理者需要申请重新评估：

- 向境外提供数据的目的、方式、范围、类型和境外接收方处理数据的用途、方式发生变化，或者延长个人信息和重要数据境外保存期限的；
- 境外接收方所在国家或者地区法律环境发生变化，数据处理者或者境外接收方实际控制权发生变化，数据处理者与境外接收方合同变更等可能影响出境数据安全的；
- 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的。

对于何谓“在实际处理过程中不再符合数据出境安全管理要求的”情形，《征求意见稿》并未给出除上述前两种情形外的进一步说明，企业在实践中数据出境场景丰富，可能经常随实际业务需求发生变化，是否任何数据出境目的、方式、范围、类型或境外处理用途、方式变化均需重新申请评估，或是在特定范围、幅度的数量变化无需申请安全评估仍有待实践检验。

五、我们的观点

《征求意见稿》对从中国向境外传输重要数据和一定规模的个人信息提出了前所未有的严格限制。将个人信息和重要数据出境的安全评估合二为一在一份规定中加以规范，体现了国家对大量个人信息出境带来的国家安全风险谨慎与担忧。

由于征求意见稿对个人信息出境政府评估设置了很低的数量门槛，而目前正在征求意见的规定和指南对重要数据的界定亦非常宽泛，如果最终稿按目前规定出台，对于那些业务依赖境外数据处理或集中存储的公司而言，为了避免冗长的评估程序和与此相伴的不确定性，数据本地化可能是一个不可避免的昂贵选择。

这不仅会给在华跨国企业带来 IT 架构调整、内部组织架构调整及随之而来的巨大前期投入成本，还将产生数据出境梳理、数据跨境传输协议管理、出境数据后续境外使用持续监管等大量持续的日常合规投入。预计可能将大量涌来的评估申请亦可能对网信办的审查能力带来压力和挑战。因此，我们呼吁监管机构在执行新规过程中，为企业合规预留一定合理的过渡期，以期企业、监管机构各方逐步落实合规要求，减少对跨国企业的业务冲击，共同实现数据合法有序自由跨境流动。

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或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com