HANKUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2021 年第 11 期（总第 175 期）

新法评述

1、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

2、快评《网络数据安全管理条例（征求意见稿）》对企业境外上市的潜在影响

新法评述

1、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：段志超丨蔡克蒙丨王雨婷[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。

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

[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）》。

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的各类客户数据、员工数据跨境传输带来较大的不确定性。

[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。

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。

2、快评《网络数据安全管理条例（征求意见稿）》对企业境外上市的潜在影响

作者：段志超丨周颖丨蔡克蒙

2021 年 11 月 14 日，国家互联网信息办公室（**“网信办”**）首次公布了《网络数据安全管理条例（征求意见稿）》（**“条例征求意见稿”**）并向社会公开征求意见。条例征求意见稿以《个人信息保护法》、《数据安全法》和《网络安全法》等法律为依据，全方位地细化了上述法律中关于个人信息和重要数据保护的规定，并回应了网信办在今年 7 月份发布的《网络安全审查办法》（征求意见稿）（**“办法征求意见稿”**）所留下的一些疑问。本文是汉坤关于条例征求意见稿的系列解读中的首期解读，将聚焦条例征求意见稿对企业境外上市的潜在影响。

一、网络安全审查要求：香港上市的优待和 100 万人个人信息触发的申报义务

此前办法征求意见稿规定第 6 条曾规定“掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”。由此带来的普遍疑问是“赴国外上市”是否包括香港上市？由于办法征求意见稿非同寻常地使用了“赴国外上市”的字眼，因此业界普遍猜测监管机构可能旨在为企业赴香港上市做出一些“优待”。

条例征求意见稿明确香港上市也可能需要申请网络安全审查。其在保留仅基于个人信息数量的赴国外上市背景下的申报网络安全审查义务的同时，对于赴香港上市作出了差异化的规定，仅规定在相应上市具有国家安全影响考量时的安全审查义务。条例征求意见稿第 13 条规定，“数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查：（一）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者[4]实施合并、重组、分立，影响或者可能影响国家安全的；（二）处理一百万人以上个人信息的数据处理者赴国外上市的；（三）**数据处理者赴香港上市，影响或者可能影响国家安全的**；（四）其他影响或者可能影响国家安全的数据处理活动……”

然而，遗憾的是条例征求意见稿并未对“影响或者可能影响国家安全的”范围和认定标准做出任何界定。如果条例征求意见稿按目前规定生效，企业出于谨慎考虑仍可能不得不事先申请网络安全审查，这可能导致上述对香港上市的“优待措施”在实践中出现效果受限的情况。

对于赴美国等国外上市的数据处理者，只要“处理一百万人以上个人信息”即必须向网络安全审查办公室申报网络安全审查。与办法征求意见稿相同，条例征求意见稿并未明确规定处理个人信息以外的其他重要数据或者核心数据处理者赴国外上市必须申请安全审查，但这类企业的国外上市也可能属于“其他影响或者可能影响国家安全的数据处理活动”而落入安全审查的范围。

值得注意的是，相较于办法征求意见稿中宽泛地将运营者都纳入上市申报网络安全审查主体的范围内，且对于 100 万用户个人信息的触发阈值使用了“掌握”这一相对模糊的概念，条例征求意见稿将上市申报网络安全审查的主体限定在“数据处理者”，即，在数据处理活动中自主决定处理目的和处理方式的个人和组织[5]。但这是否意味着将在业务过程中主要接受委托处理数据（例如云服务提供商，对于客户数据而言通

[4] 互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

[5] 条例征求意见稿第 73 条。

常并不构成条例征求意见稿意义上的“数据处理者”）的相关运营者排除在外，尚存在不确定因素，有待监管的进一步明晰。

此外，条例征求意见稿未对“上市”的概念做出澄清。对此，我们仍保持此前在办法征求意见稿出台时的观点，即除 IPO（首次公开募集股份并上市）外，中概股公司在美国上市可能采取的 SPAC（特殊目的收购公司）并购、RTO（反向兼并/借壳上市）、Direct Listing（直接上市）等方式均可能被纳入网络安全审查的范围。此外，由于中概股公司在进行香港二次上市时及上市后可能需要根据香港上市规则额外披露或提供信息，并且也将受限于香港联交所及证券监管机构的监督和调查，因此对于已经在境外上市的中概股公司而言，如赴香港二次上市存在“影响或者可能影响国家安全的”，亦将需要申请网络安全审查。

二、赴境外上市公司的年度数据安全评估及报告义务

在网络安全审查以外，条例征求意见稿亦规定了相关赴境外上市公司的数据安全评估和上报义务。第 32 条规定，处理重要数据[6]或者**赴境外上市的数据处理者**，应当**自行或者委托数据安全服务机构**每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门。我们理解，这里的**“赴境外上市的数据处理者”**似包括处在境外上市过程中的数据处理者以及已经在境外上市的数据处理者。

对于处在境外上市过程中的数据处理者，如其满足前述触发网络安全审查义务的条件的，将需要同时考虑网络安全审查义务和数据安全评估义务。对于处理个人信息相对数量较少或者不涉及国家安全考量的数据处理者，其仍需要进行相关数据安全评估，并按规定进行上报。

而对于已经在境外上市的数据处理者，仅从条例征求意见稿文义上解读，该等规定可能意味着其不会被溯及地要求重新申报网络安全审查，但无论其是否处理一百万人以上个人信息或涉及国家安全，均需要在每年 1 月 31 日向市级网信部门提交前将上一年度数据安全评估报告。

根据条例征求意见稿的规定，年度数据安全评估报告的内容包括：（一）处理重要数据的情况；（二）发现的数据安全风险及处置措施；（三）数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；（四）落实国家数据安全法律、行政法规和标准情况；（五）发生的数据安全事件及其处置情况；**（六）共享、交易、委托处理、向境外提供重要数据的安全评估情况**[7]；（七）数据安全相关的投诉及处理情况；（八）国家网信部门和主管、监管部门明确的其他数据安全情况。

---

[6] 条例征求意见稿第 73 条规定：**重要数据**是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。包括以下数据：1.未公开的政务数据、工作秘密、情报数据和执法司法数据；2.出口管制数据，出口管制物项涉及的核心技术、设计方案、生产工艺等相关的数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争实力有直接影响的科学技术成果数据；3.国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；4.工业、电信、能源、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；5.达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等人口与健康、自然资源与环境国家基础数据；6.国家基础设施、关键信息基础设施建设运行及其安全数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；7.其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。

[7] 根据第 32 条，赴境外上市的数据处理者如开展共享、交易、委托处理、向境外提供重要数据，其安全评估应当重点评估以下内容：（一）共享、交易、委托处理、向境外提供数据，以及数据接收方处理数据的目的、方式、范围等是否合法、正当、必要；（二）共享、交易、委托处理、向境外提供数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；（三）数据接收方的诚信状况、守法情况、境外政府机构合作关系、是否被中国政府制裁等背景情况，承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；（四）与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务；（五）在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险。评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、委托处理、向境外提供数据。

三、境外上市过程中重组的报告义务

条例征求意见稿还新增了对于数据处理者进行架构重组时涉及重要数据和一百万人以上个人信息时的报告义务。如相关公司在上市过程中基于各种原因需进行架构重组的，可能会需要按照相关规定进行报告。条例征求意见稿第 14 条规定，数据处理者发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告；数据处理者发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。

对于何为“**涉及**重要数据和一百万人以上个人信息的”可能有不同的解释。从狭义上理解，似乎仅因合并、重组、分立等情况导致转让或“剥离”重要数据和一百万人以上个人信息的（例如在上市重组过程中涉及业务和资产转让时，将重要数据和一百万人以上个人信息从一家主体转让至另外一家主体），才需要受此条管辖[8]。然而，从广义上理解，本条可理解为如集团内有数据处理者处理重要数据和一百万人以上个人信息的，则集团的重组（即使不涉及数据在不同主体间进行转让，或者相关数据处理者的合并或分立）也需履行报告义务。如按此理解，常见的红筹架构搭建和拆除等重组活动可能均需向网信办进行报告。

四、小结

由于条例征求意见稿延续了办法征求意见稿此前设定的“一百万人以上个人信息”较低门槛，因此事先申报网络安全审查将几乎成为涉及个人信息的企业未来申请赴美上市的“标配”。对于赴香港上市而言，虽然条例征求意见稿设定了“影响或者可能影响国家安全的”这一看似较为宽松的条件，但其具体要求仍有待监管机构在实践中明确。此外，条例征求意见稿关于赴境外上市企业的年度安全评估和报告规定以及数据处理者发生合并、重组、分立等情况时的报告规定，亦将成为相关企业在赴境外上市前以及上市后必需履行的合规义务。

[8] 原因在于第 14 条这里使用了“数据接收方”的概念，而该概念通常在数据转让的场景中使用。

特别声明

汉坤律师事务所编写《汉坤专递》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，请与汉坤律师事务所的下列人员联系：

北京　金文玉　律师：

电话：　+86 10 8525 5557

Email：　wenyu.jin@hankunlaw.com

上海　曹银石　律师：

电话：　+86 21 6080 0980

Email：　yinshi.cao@hankunlaw.com

深圳　王哲　律师：

电话：　+86 755 3680 6518

Email：　jason.wang@hankunlaw.com

香港　陈达飞　律师：

电话：　+852 2820 5616

Email：　dafei.chen@hankunlaw.com