

中国公布《数据出境安全评估申报指南》对跨国商务之影响

作者：杨迅 | 夏雨薇 | 杨蕾

2022 年 8 月 31 日晚，于《数据出境安全评估办法》(“评估办法”)生效前夕，国家网信办(“网信办”)发布了《数据出境安全评估申报指南(第一版)》(“指南”)。指南为评估办法中数据出境安全评估(“数据出境安全评估”)的方式、程序和所需材料提供了指引。

1. 适用范围

指南规定了需要进行数据出境安全评估的数据出境的范围。

与评估办法颁布时《<数据出境安全评估办法>答记者问》中对“数据出境”的回应相一致，指南中“数据出境”包括以下情况：(1)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；(2)数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出。这样看来，“数据出境”的定义十分宽泛，只要数据实际可能从中国流向境外(无论是以转移到海外服务器的方式，还是以被境外方暂时查看的方式)，那么这些数据都会被视作出境。

指南还重申了评估办法中规定的数据出境需要进行数据出境安全评估的门槛。数据处理者(“数据出境方”)在如下情况下需要申报数据出境安全评估：(1)数据处理者向境外提供重要数据；(2)关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；(3)自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；(4)国家网信办规定的其他需要申报数据出境安全评估的情形。

.....
For more Llinks publications,
please contact:

Publication@llinkslaw.com

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

尽管有指南的指引，一些关于数据出境安全评估的实际问题依然不甚清晰。譬如，依指南指引，一个处理 100 万人以上客户个人信息的数据出境方，即使其仅出境少量的员工个人信息，仍需要申报数据出境安全评估。然而，在中国境内处理客户个人信息的体量与出境少量员工个人信息有何联系？指南对此并未作出回应。

另一个有待澄清的问题是，将数据存储于境外云服务器的行为是否构成数据出境？争议点在于，当数据被保存至境外云服务器上时，可能并不存在所谓的海外接收方。尤其在于，即使是境外云服务器的供应商，也无法合法地访问上云的任何数据。然而根据指南的指示，在海外云服务器上保存数据仍被视为数据出境。这背后的依据可能是，网信办担忧当数据流向中国境外时，可能会面临在域外辖区缺乏个人信息保护的风险及域外政治风险。因此，在指南中，服务器的地理位置是数据出境安全评估时的考虑因素之一。

有鉴于此，数据处理者若将数据存储于境外云服务器上，其仍可能被视为数据出境方。因数据的跨境转移仍能引发风险，从而需纳入监管范围。由于在该类数据出境活动中并无所谓的“接收方”，数据出境方可提交云服务合同作为评估办法所要求的“法律文件”以支持申报数据出境安全评估。

2. 数据出境安全评估程序

根据指南，数据出境方必须送达书面申报材料并附带材料电子版。申报材料包括：(1)统一社会信用代码证件影印件；(2)法定代表人身份证件影印件；(3)经办人身份证件影印件；(4)经办人授权委托书；(5)数据出境安全评估申报书(“申报书”)；(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影印件(“法律文件”)；(7)数据出境风险自评估报告(“自评估报告”)；(8)其他相关证明材料。

指南中还提到，上述第 6 项和第 8 项的申报材料可以提交非中文版本，但须同步提交准确的中文译本。对大部分跨国公司而言，其多数合同都是以非中文版本签署的，上述要求虽然产生额外翻译成本，但并非不可克服。此外，指南中申报书的模板还格外要求将评估办法第 9 条中所要求的 6 项内容分别清楚地纳入法律文件中，并作出显著标识。我们理解前述条款可能会被网信办着重审查。

在程序要求方面，网信办如何进行数据出境安全评估仍然未知。指南中未对网信办处理数据出境安全评估的时间作出确定承诺。只是在评估办法中规定若数据出境安全评估时间需要从 45 个工作日延长的，将告知数据出境方预计延长的时间。

指南并未列出进行数据出境安全评估的详细流程，其既没有提到是否将向其他政府机关进行咨询，也未指明是否进行现场检查。这似乎可以被解读为，数据出境安全评估将主要基于文本审阅。而根据安全评估第 10 条的要求，网信办极有可能将引入技术机构进行技术层面的评估，并向行业主管部门征询行业监管意见。

从指南提供的申报材料的模板中解读，数据出境安全评估似乎对数据出境方以及境外接收方的数据安全能力尤为看重。例如，在自评估报告的模板中，数据出境方被要求证明其 IT 基础设施的可

靠性，包括数据出境涉及的信息系统，数据中心，出境链路，以及拟出境数据拟在境外存储的系统平台和数据中心。此外，数据出境方被要求提交其数据安全保障措施的有效性证明，例如数据安全风险评估，数据安全能力认证，数据安全检测测评，数据安全合规审计以及网络安全等级保护测评。值得注意的是，为了进一步确认自评估报告的真实性与可靠性，网信办要求进行自评估的第三方机构对其在自评估报告中包含的内容部分以加盖公章的方式进行背书。也就是说，参与完成自评估报告的主体，必须披露其姓名，并对其作出的意见承担相应责任。

3. 实质性要求

实施数据出境安全评估，实则是对数据出境方的数据与网络安全法律合规情况的全面审查。在指南中，网信办要求在数据出境安全评估阶段评估数据出境的风险时，应考虑数据出境方对数据和网络安全相关法律法规的遵守情况。包括数据出境方的合规历史记录，个人责任以及数据出境方的管理与技术体系。特别是：

- 在申报书中，数据出境方必须披露其合规历史记录，包括其近 2 年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以及整改情况，重点说明数据和网络安全方面的相关情况。
- 数据出境方应当披露数据出境方和境外接收方的数据安全负责人以及管理机构的信息，包括其姓名，联系方式，职位，国籍，证件号码。
- 数据出境方应当阐明其数据保护管理体系，包括全流程管理、分类分级、应急处置、风险评估、个人信息权益保护的情况。此外，数据出境方被要求介绍其在数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的技术措施。

这实质上意味着，遵守数据和网络安全法律法规，是通过数据出境安全评估的重要因素。

4. 实践建议

评估办法已于昨日正式生效，指南与公开咨询热线也随即公开。对日常进行数据出境活动的跨国公司而言，数据出境安全评估是不可避免的负荷。

显然，继续已有的数据出境活动，并根据法律要求进行数据出境安全评估，对跨国公司而言是行政上的沉重负荷。因此，一些跨国公司正在采取“中留中”策略，将其区域数据库部署在中国，以减少数据出境的频率和数量。

我们也意识到，跨国公司仍需为了其全球化处理出境部分数据。基于此，我们建议公司参考指南中提供的自评估报告模板，尽早建立内部的数据出境风险评估流程。将风险评估流程作为标准程序并纳入内部管理体系后，也能有效减少行政成本。

如您希望就相关问题进一步交流，请联系：



杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2022