君合专题研究报告

2022 年 7 月 11 日

中国数据出境监管实务探讨

数据出境作为中国数据合规领域的重要话题，自 2016 年《网络安全法》出台之后即成为合规热点。2021 年《数据安全法》和《个人信息保护法》相继实施后，对于数据出境合规的讨论热度持续升温。数据出境涉及的监管要求有其尚未明确之处，但对于从事跨境业务或是面临现实数据跨境流转需求的企业来说，如何以合理的合规成本实现有效的风险防控，是企业在数据隐私与网络安全领域始终面临的课题之一。

随着近日《数据出境安全评估办法》、《个人信息出境标准合同规定（征求意见稿）》等相继发布，选择可行的数据和个人信息出境机制、制定适合企业自身特点的数据出境合规方案整体有了更加清晰的思路。本文拟从我国数据出境的最新监管规则体系出发，结合我们多年与企业客户并肩摸索的实务经验和理解，就数据出境监管的实务场景和出境机制的构建思路进行探讨与分享。

一、数据出境的监管框架

自《网络安全法》对关键信息基础设施者提出重要数据和个人信息的境内存储和出境安全评估要求以来，有关数据出境的前提条件、出境机制、评估要求在 2017 年后陆续发布。从现有规则体系来看，除《网络安全法》《数据安全法》《个人信息保护法》外，其他下位法规或标准文件多为征求意见稿或待生效阶段。尽管尚未正式实施，多份规则中的细节规定为数据出境工作的开展提供了较大参考价值。为便于系统理解我国数据出境监管规则体系的立法的重点和变化，我们将主要法规和标准文件概述如下。

1. **《网络安全法》**（2017.6.1 生效）

- 第 37 条规定关键信息基础设施运营者在中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，应按照有关办法进行安全评估。

2. **《数据安全法》**（2021.9.1 生效）

- 第 31 条规定关键信息基础设施运营者的数据出境安全管理依照《网络安全法》的相关规定；对于其他数据数据处理者在中国境内运营中收集和产生的个人信息和重要数据的出境安全管理办法，另行制定。针对境外司法、执法机构关于提供数据的请求，第 36 条规定境内的组织、个人必须经过中国主管机关批准，方可向境外司法、执法机构提供存储于中国境内的数据。

3. **《个人信息保护法》**（2021.11.1 生效）

- 第 38 条规定了个人信息处理者因业务等需要，确需向中国境外提供个人信息时应符合的条件，包括通过（1）国家网信部门组织的安全评估；（2）经专业机构进行个人信息保护认证；（3）按照国家网信部门制定的标准合同与境外接收方订立合同；（4）法律、行政法规或者国家网信部门规定的其他条件。

- 第 39 条对个人信息处理者向境外提供个人信息的其他条件，包括告知和取得单独同意。
- 第 40 条对于关键信息基础设施运营者和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，规定了个人信息本地化存储的要求，确需向境外提供的，应当通过国家网信部门组织的安全评估。
- 针对境外司法、执法机构关于提供个人信息的请求，第 41 条规定了境内的组织、个人必须经过中国主管机关批准， 方可向境外司法、执法机构提供存储于中国境内的个人信息。
- 第 55 条规定向境外提供个人信息前，需进行个人信息保护影响评估。

4. **《数据出境安全评估办法》**（2022.9.1 生效）

- 该办法正式发布了重要数据和个人信息出境的安全评估要求，指出评估包括事前评估和持续监督。
- 同时该办法也规定了评估流程、重点评估事项、申报要求、评估周期，以及对已经开展的数据出境活动提出了 6 个月内完成整改的要求。

5. **《个人信息和重要数据出境安全评估办法（征求意见稿）》**（2017.4.11 发布）

- 该办法对个人信息和重要数据这两种数据类型的出境安全评估规则进行了规定，包括数据安全评估的适用情形、自评估要求、安全评估重点、主要流程等。
- 相关数据出境安全评估的相关内容已由即将生效的《数据出境安全评估办法》替代。

6. **《个人信息出境安全评估办法（征求意见稿）》**（2019.6.13 发布）

- 该办法针对个人信息出境安全评估机制进行了具体规定，包括个人信息出境安全评估需提供的材料、主要评估流程、个人信息出境记录记录要求等。
- 由于个人信息出境安全评估的相关内容已由此后发布的《数据出境安全评估办法（征求意见稿）》替代，该办法参考价值可能有限。

7. **《数据安全管理办法（征求意见稿）》**（2019.5.28 发布）

- 该办法第 28 条规定，网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经相关监管部门同意。

8. **《网络安全审查办法（2021）》**（2022.2.15 生效）

- 第 7 条规定，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

9. **《网络数据安全管理条例（征求意见稿）》**（2021.11.14 发布）

- 该条例以专章的形式细化了数据跨境安全管理规则，其中重点规则包括（1）第 35 条对数据处理者向中国境外提供数据的前提条件规定；（2）第 36 条对《个人信息保护法》第 39 条的规定的重申（但明确收集个人信息时已单独就个人信息出境取得个人同意，且按照取得同意的事项出境的，无需再次取得个人单独同意）；（3）第 37 条规定了应当通过数据安全评估的情形的规定；（4）第 40 条对向境外提供个人信息和重要数据的数据处理者规定了编制数据出境安全报告义务的要求。

10. **《数据出境安全评估办法（征求意见稿）》**（2021.10.29 发布）

- 该办法对数据安全评估机制的具体实施规则进行了规定，包括申报条件、自评估要求、需提交的材料、评估重点、评估流程等内容。
- 相关数据出境安全评估的相关内容已由即将生效的《数据出境安全评估办法》替代。

11. **《个人信息出境标准合同规定（征求意见稿）》**（2022.6.30 发布）

- 该规定对《个人信息保护法》下签订标准合同这一个人信息出境机制进行了较为全面的制度安排，包括适用标准合同的前提条件、个人信息保护影响评估的重点评估内容、标准合同的主要内容、标准合同的备案要求、重新签订标准合同的情形以及行政处罚等法律后果。

12. **《信息安全技术 个人信息安全影响评估指南》**（2021.6.1 生效）

- 该指南对个人信息安全影响评估机制进行了详细的介绍，指出评估步骤应包括必要性分析、评估准备工作、数据映射分析、风险源识别、个人权益影响分析、安全风险综合分析、评估报告撰写、风险处置和持续改进、制定报告发布策略等。
- 同时，该指南的附录还对部分个人信息处理活动的安全评估要点进行了列举，但未包括个人信息出境这一场景。

13. **《信息安全技术 数据出境安全评估指南（征求意见稿）》**（2017.8.30 发布）

- 该指南对数据出境的定义和情形进行了较为详细的规定，不仅包括数据物理出境的情形，还包括数据虽未转移存储至中国境外，但仍可能被认定为出境的情形，对实践中数据出境行为的判断具有一定参考价值。
- 相关数据出境安全评估的相关内容已由即将生效的《数据出境安全评估办法》替代。

14. **《网络安全标准实践指南 个人信息跨境处理活动安全认证规范》**（2022.6.24 发布）

- 该规范为认证机构对个人信息跨境处理活动进行保护认证的基本要求，规定了个人信息保护认证这一个人信息出境机制的适用情形、认证主体及基本要求。
- 基本要求涵盖了有法律约束力的协议、组织管理、个人信息跨境处理规则、个人信息保护影响评估等方面。同时该文件还强调了认证机制对个人信息主体权益保障的重视。由于该文件并非国家网信部门发布，个人信息处理者能否依据该规范满足《个人信息保护法》规定的个人信息保护认证要求，从而合法地向境外传输个人信息，需进一步探讨。

二、实务场景概述

在实践中，由于企业所在行业和主营业务以及监管要求的差异，数据出境的具体场景也比较多。结合我们近年协助不同行业客户处理涉外项目和案件中的数据出境事宜，我们将实务过程中高频出现，且在处理方式上相对有挑战性的场景概括为以下几类。需注意的是，在下述场景中，数据出境不仅包括向境外传输、存储境内数据（例如邮件发送、上传至境外服务器），也包括未转移数据但为境外主体提供访问或调用权限等方式。在个别场景下，在境内向境外机构展示或允许其在境内查看境内的数据或文件信息，也有可能涉及“数据出境”的合规问题。

场景一：跨国企业集团对业务和人事数据的全球化管理

- 跨国企业集团因业务或管理需要，向境外集团总部、同一集团内的关联公司或其他第三方提供境内收集或产生的经营数据、产品或服务的用户信息、员工信息、财务数据等，以便境外公司进行管理或分析。其中员工信息的提供除为统一的劳动用工管理目的外，也有可能在员工违纪调查等事项中涉及，例如将含有员工个人信息的调查报告发送给境外管理层。

场景二：境外企业因业务开展对境内数据的收集

- 部分已在或未在境内设立运营实体的企业可能因业务开展需要，直接或间接从中国境内收集数据，例如向境内用户提供产品或服务时对用户交易信息的收集。

场景三：企业在涉外诉讼中的文件披露与证据开示

- 境外诉讼案件中的证据开示程序有可能要求境内企业或外国公司和/或其国内关联方，作为案件当事人或第三人的角色，收集并提供与案件相关的材料证据（除非受到律师-客户特权的保护）。未能响应或配合证据开示要求的企业有可能面临境外诉讼案件中的不利地位影响或面临法院的处罚。

场景四：企业面对跨境调查或境外制裁时的配合

- 外国政府机构（例如美国司法部、财政部等）基于其管辖权可能对境内企业发起反腐败、出口管制、反洗钱等领域的调查。在收到此类调查通知后，企业在多数情况下会首先启动内部调查程序，根据调查目标和配合要求收集并筛查涉案文档资料、证据信息等。未能配合调查披露文件信息的企业有可能面临适用的外国法规对其认定违规事项的处罚或制裁措施。

场景五：境外上市企业的数据披露要求

- 境外上市的中国企业需按照当地法律或监管机构要求披露企业信息，或提交可供检查的审计底稿和企业内部资料。无法满足信息披露要求或响应审计检查要求的企业则可能面临退市风险。

以上场景暂未讨论涉及特定行业或情形下的特殊情况（如涉及健康医疗行业的临床数据出境问题），实践中，对于数据出境在现实情况下需要考虑的问题和可能遭遇出境限制的环节会受到不同因素的影响。

总体来说，企业面临的数据出境场景可以大致划分为商事场景和司法执法场景两大类。在商事场景中，企业对自身数据合规义务的识别与分析，除了保障数据出境的顺利进行，也有助于防范违法违规风险，避免给企业带来处罚、侵权诉讼、商誉损失等不利影响。而司法执法场景对于多数企业来说可能不常见，一旦遭遇，其处理难度和成本相较商事场景将大大提高，数据出境的可行性判断、出境要求和限制的识别、出境机制的设计将更为复杂棘手，很多时候需要结合司法执法问题所涉及的法律问题本身、国家安全要求、数据出境限制、个人信息保护基础、以及域外法律冲突、国际礼让原则等进行通盘考虑，制定解决方案。

三、构思数据出境方案的思路和维度

结合我们的经验，针对上文提及的实务场景，企业在分析自身法律义务并构思恰当的数据出境机制时，常见的工作步骤包括：（1）梳理确定具体的业务场景（如依托的商业场景）、数据出境的目的和必要性；（2）盘点分析不同场景中企业数据处理角色、数据流转情况、企业现有制度政策、特定法域的要求等；（3）识别企业的法律合规差异、应满足的出境机制和条件（如安全评估、安全认证、标准合同或法律文件签订、监管备案、安全技术措施等）、待履行义务和违规后果；（4）针对前述差异和义务要求，制定行数据出境方案（包括出境机制、合规方案、数据处理协议等）、区分事项优先级，组织相关部门实施行动计划。前述思路和步骤是较为通用的描述，整体数据出境方案的设计和构思可结合下三个维度做细节调整。

1. 出境主体

就数据出境主体而言，不同类型的主体在国内法下面临的数据出境限制和要求存在差异。例如《网络安全法》第 37 条要求，关键信息基础设施运营者境外提供境内收集和产生的个人信息和重要数据应当在境内存储，因业务需要确需经向外提供的，需依法进行安全评估。再如 2022 年初生效的的《网络安全审查办法》第七条规定，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。此外，日前发布的《个人信息出境标准合同规定（征求意见稿）》也对合同模板的适用范围明确了适用条件，排除了关键信息基础设施运营者，处理个人信息或向境外提供个人信息达到一定数量级的个人信息处理者选择签订标准合同为数据出境机制的可能性。

2. 数据类型

数据出境可行性判断和出境机制的设计也需要将拟出境的数据类型纳入考量范围。根据我们对

已出台法规和实践案例的了解，受到出境禁止或限制要求、或应满足特定审批/评估要求，抑或是企业自身有保护需求的数据类型主要包括：（1）个人权益保护：个人信息、敏感个人信息、个人隐私等；（2）安全保密：国家秘密、核心数据、重要数据、涉密档案资料；（3）跨境监管：审计工作底稿、会计档案、证券业务有关文件资料等；（4）行业要求：医疗数据、人口健康信息、金融征信数据、汽车数据等；（5）其他：商业秘密、保密商务信息等。

3. 接收对象

接收对象的考虑主要与外国司法、执法机构的数据提交要求有关。这一类型的数据出境要求时常出现在涉外诉讼、政府调查、监管检查等场景中，根据《个人信息保护法》第 41 条或是《数据安全法》第 36 条规定，未经主管机关批准，境内组织或个人直接向外国司法或执法机构提供存储于境内的个人信息或数据会引发行政或刑事责任。类似的规定在《证券法》中也有提及。

在出境数据的直接或间接接收对象属于外国司法或执法机构的情形中，除了企业自身的及时响应，很多时候也需要通过组建合适的工作团队（包括境内外具有执业资格的律师、审计师等顾问），综合分析企业面临的跨境诉讼、调查或审计要求，合理确定对司法、执法机构的数据信息披露要求响应方式。

四、 执两用中的实际选择

就数据出境的国内监管而言，根据出台法规选择某项数据出境机制也非一劳永逸。由于数据出境机制存在一定的适用范围和前提，数据合规领域监管规则的升级或细化，以及实务场景中设计的具体技术措施变化，都会影响企业在具体实务场景中的判断。以签署标准合同条款为例，结合我们协助客户落地 GDPR 下标准合同条款的经验来看，满足出境机制的法律监管要求并不是简单地套用模板或是填写申请即可解决的问题。问题可能出现在标准合同签署主体的选择、数据流转的识别和描述、安全风险的实际判断、数据处理方案的调整等不同环节。

对于数据出境需求较大、处理数据类型繁多、供应链构成复杂、或是处于涉外诉讼或调查案件中的企业来说，其所面临的数据出境问题往往是两难境地，在决定向境外提供数据信息前需要考虑的问题包括是否需要响应境外的数据出境要求？是否存在必须满足的境内数据出境监管法规要求？如何满足这些要求？以及满足这些要求是否与境外监管规则存在冲突？如果存在冲突，应当如何解决？

我们期待国内数据出境监管规则的细化和正式施行对于以上问题的解答给出指导。对于现阶段存在实际数据出境需求或面临数据出境难题的企业来说，不妨考虑基于现有监管规则与发展趋势，结合企业所面问题的紧迫程度、风险承受能力与法律合规资源，通过保持与监管机构的沟通、整合内部流程、就数据出境安全评估等即将生效的法规要求开展落地准备工作，来规划符合企业自身特点和需求的合规解决方案。

孙博　合伙人　电话：86- 21 22086216　邮箱地址：sunb@junhe.com
马晓媛　律　师　电话：86- 21 22086114　邮箱地址：maxiaoyuan@junhe.com