数据跨境现状调查与分析报告

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

南财合规科技研究院 SFC Compliance Technology Institute

数据跨境现状调查与分析报告

——基础问题与十个痛点的解决

目录

上篇：基础问题篇

一、 我国有哪些数据跨境相关的法律法规要求?

随着数字化成为我国重要的国家战略，数据正逐渐被我国政府视为保障国家主权、对国家安全和经济发展具有重大影响的重要资产。监管部门对数据跨境传输的合规情况亦越发关注。

自 2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》(下称《网络安全法》)、2021 年 9 月 1 日起施行的《中华人民共和国数据安全法》(下称《数据安全法》) 和 2021 年 11 月 1 日起施行的《中华人民共和国个人信息保护法》(下称《个人信息保护法》)，均从法律层面对开展数据出境活动进行了规定。我国立法针对数据出境采用了"分层监管"的方式，即将关键信息基础设施运营者与一般网络运营者进行区分监管。

企业应当根据自身属性和出境数据的类型与性质的不同，判断需要相应承担的不同层次数据出境合规义务。从自身属性角度看，当数据出境主体构成关键信息基础设施运营者时，在境内运营期间收集和产生的个人信息与重要数据的出境活动是存在限制的；从数据类型角度看，个人信息、重要数据、国家核心数据、以及由特别法管辖下的特殊类型数据，则需要适用不同的出境规则。(具体内容请见《下篇：调查分析篇》"如何准确识别数据跨境传输的类型"部分)

为推动法律落地，在行政法规层面，国家互联网信息办公室（下称"网信办"）及相关中国数据保护和网络安全监管机构也陆续发布了一系列的规章、国家标准和指南等文件。网信办于 2021 年 11 月 14 日发布了《网络数据安全管理条例（征求意见稿)》(下称《网数条例（征求意见稿)》)，设专章对"数据跨境安全管理"作出具体规定，其正式稿也有望于今年出台；在部门规章层面，2022 年 9 月 1 日施行的《数据出境安全评估办法》对哪些数据出境主体需要申报数据出境安全评估以及申报的要求作出了规定，与之配套出台的《数据出境安全评估申报指南（第一版)》(下称《指南（第一版)》) 对申报材料的具体要求作出了指引(具体内容请见《下篇：调查分析篇》"如何完成数据出境安全评估"部分)。网信办于 2023 年 2 月 24 日发布、将于 2023 年 6 月 1 日施行的《个人信息出境标准合同办法》(下称《标准合同办法》)，对数据出境主体向境外提供个人信息时在何种条件下才应与境外接收方签订标准合同作出了规定，同时也提供了标准合同模板(具体内容请见《下篇：调查分析篇》"如何评估跨境传输相关法律文件完善程度"部分)。此外，全国信息安全标准化技术委员会（TC260）(下称"信安标委") 于 2017 年 8 月 25 日发

布了《信息安全技术 数据出境安全评估指南（征求意见稿）》（下称《安全评估指南（征求意见稿）》），在网信办未发布《数据出境安全评估办法》前规范数据出境安全评估流程、评估要点、评估方法等内容。同时信安标委在《个人信息跨境处理活动安全认证规范》（TC260-PG-20222A）的基础上于 2022 年 12 月 16 日发布了更新版本《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 V2.0》（下称《认证规范 V2.0》）。该认证规范旨在明确该认证机制的适用情况、专业机构认证的依据以及通过认证需要遵守的规则。

虽然上述法规、办法、标准中尚有个别未最终发布或生效，但这一系列文件为中国监管机构（如网信办、中国证监会）在审查数据跨境传输活动和境外上市企业时提供了参考依据。由此可见，涉及跨境传输数据的企业正面临新一轮合规挑战—在没有形成统一规则、缺乏最终清晰指引的情况下，其需要花费时间成本、人力、物力不断完善多个业务线或部门的工作流程、调整现有的全球数据战略规划、创建新的数据存储解决方案并修改或起草相关制度及合同文本等。

二、 哪些行为属于数据出境?

网信办于 2022 年 8 月 31 日发布的《指南（第一版）》第一部分"适用范围"中对属于"数据出境"的行为做出了描述，将数据跨境传输的场景归纳为三种行为：

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；及

3.网信办规定的其他数据出境行为。

（具体内容请见《下篇：调查分析篇》"如何准确识别数据跨境传输场景"部分）

三、 哪些情况下需要开展数据出境安全评估?

根据《数据出境安全评估办法》第四条，有下列情形之一的，应当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.国家网信部门规定的其他需要申报数据出境安全评估的情形。

（具体应如何判断请见《下篇：调查分析篇》“如何确认采取哪种出境安全保障机制”部分）

四、 什么数据是重要数据？现阶段识别重要数据的参考依据有哪些？

《数据安全法》首先提出了建立国家安全观以及数据安全制度体系，要求国家数据安全工作协调机制统筹协调制定国家重要数据目录，加强对重要数据的保护。因此，“什么是重要数据”以及“如何识别重要数据”成为影响当前国家数据安全工作进展的重大议题。《数据出境安全评估办法》第十九条也对重要数据进行了定义，即重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

信安标委于 2022 年 1 月 13 日公布了调整后的《信息安全技术 重要数据识别指南（征求意见稿）》。2022 年 4 月 26 日，曾有专家在公众号发布《信息安全技术 重要数据识别规则（征求意见稿）》（下称《重要数据识别规则（征求意见稿）》），作为《信息安全技术 重要数据识别指南（征求意见稿）》的最新过程稿，其划分了重要数据的定义范围，规定重要数据是指“特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全”。并且，《信息安全技术 重要数据识别规则（征求意见稿）》指明识别重要数据的基本原则、明确重要数据的识别因素等，不仅为各行业、地区、部门制定本行业、本地区、本部门的重要数据具体目录提供参考，也为企业识别其自身掌握的重要数据提供实践指引，从而进一步为国家重要数据安全保护工作提供支撑。

工业和信息化部（下称“工信部”）也于去年底开始开展工业领域数据安全管理试点，其中要求试点企业按照《工业数据分类分级指南（试行）》《工业领域重要数据和核心数据识别规则（草案）》开展数据分类分级，制定重要数据清单，并向主管部门报备。

（关于如何识别与界定重要数据具体内容请见《下篇：调查分析篇》“如何准确识别跨境传输数据的类型”部分）

五、 如何识别关键信息基础设施及其运营者？如何针对相关数据进行评估？

（一）识别关键信息基础设施（下称“CII”）和关键信息基础设施的运营者（下称“CIIO”）的法律依据有哪些？

根据目前的立法现状，关于识别和认定 CII 和 CIIO 方面，企业可以综合参考《网络安全法》、由国务院发布并于 2021 年 9 月 1 日施行的《关键信息基础设施安全保护条例》（下称《保护条例》）、公安部于 2020 年发布的《贯

彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（下称《指导意见》）、网信办网络安全协调局于 2016 年 6 月公布的《国家网络安全检查操作指南》，以及 2020 年 8 月发布的国家标准《信息安全技术关键信息基础设施边界确定方法（征求意见稿）》（下称《CII 边界确定方法》）。

（二）判断关键信息基础设施的运营者的思路及方式是什么？

一般而言，通过以下三个步骤识别 CIIO：

1.判断所涉业务是否涉及重要行业和领域

根据《网络安全法》第三十一条，CII 所涉的重点行业和领域包括：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，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、公共利益的行业和领域。《保护条例》第二条则在《网络安全法》的基础上进一步补充，提出 CII 范围包括："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、国防科技工业等重要行业和领域，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、公共利益的重要网络设施、信息系统等。"

此外，根据公安部发布的《指导意见》，"基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象"有可能会被纳入 CII。

因此，不难看出，国家针对 CII 所涉行业和领域的划分采用的是非穷尽列举式抽象定义，并以"视具体情况认定重点行业和领域"的情形留有余地。

2.识别关键业务及具体关键信息基础设施

在初步确认所涉业务可能会被认定为属于上述重要行业和领域之后，企业可以依据《CII 边界确定方法》进一步评估其是否存在"一旦遭到破坏或者丧失功能，会严重危害国家安全、经济安全、社会稳定、公众健康和安全的"、并且依赖信息化运行的业务，来识别、筛选关键业务。即当一个企业的属性落入到第（1）点所列法规要求的 CII 所涉及的重点行业时，也不是该企业中的所有信息系统都是 CII 的范围。只有所列行业中的相关企业其高度支撑信息化运行且该系统的运行如果遭到破坏或者功能丧失有严重危害国家安全、经济安全、社会稳定、公众健康和安全后果的才有可能被纳入 CII 的范围。

在初步判断后，企业可以参考《保护条例》第九条来进一步梳理企业中"对本行业、本领域关键核心业务""重要的""一旦遭到破坏、丧失功能或者数据泄露对国家安全、社会稳定带来危害"的网络设施、信息系统；而该网络设施、信息系统则极大可能会被认定为 CII。

3.明确 CIIO

顺接上述第（2）点，需要进一步明确的是，支撑同一关键业务的 CII 可能属于一个运营者，也可能分属于多个运营者。因此，在识别出关键业务和 CII 之后，应当根据关键业务对信息化的依赖程度和依赖关系进行系统评估，梳理支撑同一关键业务的 CII 分布和运营情况，以明确对应到具体的 CIIO。

需要提醒的是，从《网络安全审查办法》《指导意见》到《保护条例》，均明确了 CII 及 CIIO 的认定工作由各自行业的主管部门负责，所以企业是否属于我国认定的 CIIO 主要取决于主管机构的判定和通知。同时，考虑到 CII 的定义以及范围均比较宽泛，并且技术以及网络安全的要求会不断地更新迭代，主管机构对于行业内企业所拥有的 CII 具体情况应该也是在一个持续的了解和动态认定的过程中，所以希望公司时刻保持关注。

（三）如果外国公司在中国投资设立的公司（下称"FIE"）被认定为 CIIO，该 FIE 的个人信息出境活动应如何开展？是否可以直接向境外母公司传输个人信息？

应当说明的是，我国现行有效的法律对于 CIIO 的个人信息出境活动（包括跨境传输员工个人信息的行为）有明确规制。《网络安全法》第三十七条规定了 CIIO 向境外提供数据的安全评估义务。《个人信息保护法》第四十条进一步规定，CIIO 应当将在中华人民共和国境内收集和产生的个人信息存储在境内。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。因此，若 FIE 被认定为 CIIO，则需要将在中国境内收集的个人信息存储在境内；如 FIE 确需向位于境外的母公司提供在境内运营中收集产生的个人信息的，应当根据《数据出境评估办法》通过国家网信部门组织的安全评估。在未履行上述要求的情况下，公司直接向境外母公司传输个人信息是存在合规风险的，可能会被要求承担上篇问题十四中所述的相关责任。

六、 哪些个人信息出境情形需要申报数据出境安全评估?

首先，企业应当识别出境数据中是否含有个人信息—根据《个人信息保护法》，个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。此外，《信息安全技术 个人信息安全规范》（GB/T 35273—2020）作为推荐性国家标准，其附录 A 列举了部分个人信息类型，附录 B 列举了部分敏感个人信息类型，均可作为判断出境数据中是否含有个人信息的依据。（具体内容请见《下篇：调查分析篇》"如何准确识别跨境传输数据的类型"部分）。

其次，企业应当结合法律要求判断自身是否属于以下情形：

第一，处理 100 万以上个人信息的数据处理者向境外提供个人信息。

《个人信息保护法》第四十条规定，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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。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。

《数据出境安全评估办法》与其上位法保持一致，并进一步就《个人信息保护法》第四十条所提及的"数量"进行了明确。

由此可见，对于处理 100 万以上个人信息的处理者，法律法规规制的对象是某一类个人信息处理者，而非某一类处理行为。如处理 100 万以上个人信息的数据处理者确有需要向境外提供个人信息，则不论向境外提供的数据量为多少，都应当事先通过国家网信部门组织的安全评估。

第二，累计向境外提供 10 万人个人信息的数据处理者或者 1 万人敏感个人信息的数据处理者。

去年 9 月起施行的《数据出境安全评估办法》明确了"10 万人个人信息或者 1 万人敏感个人信息"的起算时间，即从上年 1 月 1 日起。这一点也在《标准合同办法》中得以体现。

《数据出境安全评估办法》对此情形中的两个数量门槛设置较低，企业（尤其是跨国公司）很容易达到该标准进而被纳入需要申报数据出境安全评估的范围中，这体现了国家对于数据出境的管控日趋严格。我们建议企业尽快开展自查，充分了解内部已经累计向境外提供的个人信息数据量及流转情况，判断是否达到了上述规定的标准或者还有多少余量将可能需要申请出境安全评估。

需要注意的是，所述的"10 万""1 万"，是指实际累计向境外传输个人信息所对应主体的人数，而非指人次。例如某公司向境外传输员工个人信息，通常需要考虑加上未来新入职的员工人数，以及已经传输过的离职人员的数量，如果从去年 1 月 1 日起累计向境外已传输超过 10 万名员工，或者从去年 1 月 1 日起向境外传输 1 万名员工的敏感个人信息（如身份证号码），则该公司应当在去年 9 月 1 日《数据出境安全评估办法》生效后考虑申报数据出境安全评估。

需要注意的是，网信部门在收到申报材料后开展的数据出境安全评估与企业在提交数据出境安全评估前实施和开展的个人信息保护影响评估和数据出境风险自评估在性质上是不同的，不可混为一谈。（具体内容请见《下篇：调查分析篇》"如何确认采取哪种出境安全保障机制"部分）

七、 如何定义出境数据的“境外接收方”？

如上篇问题二中所介绍的，即使数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看或调用的（公开信息、网页访问除外），属于数据出境；同理，国内企业聘用的境外服务供应商通过境外服务器收集产生于中国境内的个人信息，也是属于数据出境。"境外接收方"一般仅指向第一手境外接收方，数据再传输活动涉及的第三方境外接收方所在国家或地区的相关情况一般不需要评估。涉及多个境外第一手数据接收方时，需在自评估

报告中结合业务场景，根据数据出境规模、涉及国家或地区的风险程度等因素，分别评估各接收方所具备的数据安全保障能力。

结合我们的经验，从跨国企业和其供应商的关系看，一般跨国企业和其聘用的供应商多为委托处理关系，还大多属于跨国公司总部直接委托境外供应商、签署数据处理协议的情况（约定跨国企业及各分支机构均为数据处理者，供应商为受托方）。当从中国境内收集或者在境内产生的数据被传输给境外供应商后，如果境外母公司可以自行查阅、浏览存储于境外服务供应商于境外服务器的中国子公司的数据，并且境外母公司供应商服务合同的相对方可以根据自己的目的进行处理（即以个人信息处理者的身份对中国境内生成的个人信息进行处理），则中国子公司实质是将个人信息出境传输至其境外母公司（即使出境的数据存储于境外服务供应商于第三国的服务器），境外母公司属于数据处理者角色的境外接收方。

八、 哪些属于“法律、行政法规另有规定，依照其规定进行评估/批准”的情况?

除《网络安全法》《数据安全法》和《个人信息保护法》确立的数据和网络安全整体体系外，企业还应当考虑其他相关法律法规的要求。例如，根据《中华人民共和国保守国家秘密法》第三十条，机关、单位对外交往与合作中需要提供国家秘密事项，或者任用、聘用的境外人员因工作需要知悉国家秘密的，应当报国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门批准，并与对方签订保密协议。如涉及健康医疗大数据，则根据《国家健康医疗大数据标准、安全和服务管理办法（试行）》第三十条，应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。如涉及测绘成果，则根据《中华人民共和国测绘法》第三十四条，属于国家秘密的，适用保密法律、行政法规的规定；需要对外提供的，按照国务院和中央军事委员会规定的审批程序执行。如涉及人类遗传资源信息，则根据《中华人民共和国生物安全法》第五十七条，向境外组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院科学技术主管部门事先报告并提交信息备份。

九、 符合条件的企业应当向哪个/些机构申请数据出境安全评估?

《数据出境安全评估办法》第四条明确，数据处理者向境外提供数据，应当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。

根据《数据出境安全评估办法》第十条，国家网信部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。可见，《数据出境安全评估办法》保留了一定的灵活性，网信办可以根据实际情况组织相关行业主管部门参与出境安全评估。

十、 数据出境安全评估流程是怎样的，需要多长时间?

根据《数据出境安全评估办法》第七条、第十二条、第十三条的要求，《数据出境安全评估办法》中的整体评估时长为 57+N 天（N 代表补充材料审核时间）；如涉及复评的，则为 72+N 天。

在整体评估流程中，《数据出境安全评估办法》第十一条还新增了数据处理者拒不补充或拒不更正材料的后果，即安全评估过程中，国家网信部门可以要求数据处理者补充或者更正材料，如数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。

此外，《数据出境安全评估办法》第十三条为数据处理者提供了救济方式。对评估结果有异议的，数据处理者可以在收到评估结果 15 个工作日内向国家网信部门申请复评，该复评结果则为最终结论。（具体内容请见《下篇：调查分析篇》"如何完成数据出境安全评估"部分）

十一、 符合条件的企业申请数据出境安全评估时，应当准备哪些申请材料?

根据《数据出境安全评估办法》第六条，申报数据出境安全评估，应当提交以下材料：

1.申报书；

2.数据出境风险自评估报告；

3.数据处理者与境外接收方拟订立的法律文件；

4.安全评估工作需要的其他材料。

具体应如何准备相关申报材料，可参考网信办发布《指南（第一版）》中的要求。

十二、 数据处理者与境外接收方拟订立的法律文件与个人信息出境标准合同有何区别?

《数据出境安全评估办法》第九条与《标准合同办法》附件"个人信息出境标准合同"[1]，分别对数据处理者与境外接收方拟订立的法律文件的内容和个人信息出境标准合同的订立要求作出了规定。需要注意的是，根据《标准合同办法》第六条，标准合同应当严格按照网信办制定版本订立，个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。当需要进行数据出境安全评估时，我们建议企业在起草与境外接收方拟订立的相关法律文件（如《数据跨境传输协议》）时，一方面应当完全按照《标准合同办法》中"个人信息出境标准合同"模板，另一方面也应当按照《数据出境安全评估办法》第九条额外提及的要点重点补充如下两种情形下的处理措施：（1）境外接收方实际控制权或者经营范围发生实质性变化；（2）接收方所在地网络安全环境发生变化或发生其他不可抗力的情形。

还应关注的是，网信办有关负责人就《数据出境安全评估办法》答记者问时，建议在法律文件中注明此文件须在通过数据安全评估后方可生效，以避免因出境安全评估未通过而造成合同主体的损失。

十三、 完成数据出境评估后，有效期为多久？什么情况下需要再次申请安全评估?

根据《数据出境安全评估办法》第十四条，数据出境安全评估的结果有效期为两年，自评估结果出具之日起算。换言之，有效期两年是指在同一数据出境目的、方式、范围、类型和境外数据接收方类型不变等情况下，不需要针对这些情况重新申请评估；当两年有效期届满，则应在有效期届满 60 个工作日前重新申报评估。

十四、 应申请安全评估但未申请出境数据，有何罚则?

《数据出境安全评估办法》没有额外规定违规责任与惩罚措施，而是援引了《网络安全法》《数据安全法》《个人信息保护法》的相关罚则。同时，若数据处理者构成犯罪的，将依法追究刑事责任。

根据《网络安全法》第六十六条，关键信息基础设施的运营者违反规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处 5 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

根据《数据安全法》第四十六条，违反规定向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下

[1] http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm

罚款；情节严重的，处 100 万元以上 1,000 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款。

根据《个人信息保护法》第六十六条，若企业违法处理个人信息，例如未在出境前进行安全评估，则可能面临最高 5,000 万元以下或者上一年度营业额 5%以下罚款、停业整顿、吊销相关业务许可或者吊销营业执照等严厉的处罚措施；同时，针对直接负责的主管人员和其他直接责任人员，也有可能被处以 10 万元以上 100 万元以下罚款，并在一定期限内禁止担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

十五、 还有哪些应当注意的具体事项?

根据《中华人民共和国保守国家秘密法》，违反法律规定存在国家秘密出境行为的，则有可能构成犯罪并依法追究刑事责任。

除此之外，企业还应当关注《中华人民共和国刑法》（下称《刑法》）规定的刑事责任，如《刑法》第一百一十一条规定，为境外窃取、刺探、收买、非法提供国家秘密、情报罪，规定了为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密或者情报的，处五年以上十年以下有期徒刑；情节特别严重的，处十年以上有期徒刑或者无期徒刑；情节较轻的，处五年以下有期徒刑、拘役、管制或者剥夺政策权利。

若涉及某特定领域或行业，公司还需要根据部门规章以确认是否存在相应的特殊规定以及罚则以及具体的处罚后果。

下篇：调查分析篇

为了解当下境内企业数据跨境的现状与困境，我们向 25 家涉及数据跨境的企业或机构发放了调查问卷，截至 2023 年 2 月 22 日回收问卷 21 份。其中，一半企业为互联网企业，5 家企业来自批发零售行业，两家来自制造业，两家为车企，其他企业则分布在科研、金融、教育等行业领域。在此基础上，研究团队还就数据跨境的具体问题与其中的九家企业及机构进行了访谈，以期对数据跨境实践中的难点与解决之道有更具深度与实操性的分析。

一、 如何准确识别数据跨境传输场景

此次研究团队回收的问卷中，有 9 份来自跨国企业，有超过 60%的参与调研企业数据跨境都采用"端到端传输"（由境内服务器向境外服务器传输）的方式，且有 16 家受访企业都明确表示公司的数据出境正在或已经按照相关法律法规要求进行了安全评估等相关工作；但另一方面，有超过一半的受访企业都表示在相关工作中面临着"公司业务和合规要求间存在冲突，难以短时间内调和"的困难，半数的企业认为"处理评估、整改和申报相关手续及流程的时间周期过长，对业务开展造成影响"；有超过三成的受访企业认为，"履行评估、整改和申报义务所花费的经济成本较高，企业难以承受"。

作为最早一批聚焦出海业务的企业之一，汇量科技对数据出境已形成一套较为成熟的经验。汇量科技在访谈中表示，很多涉及数据出境的企业多面临专业知识缺乏，难以评估数据跨境风险和控制措施的有效性的现状。

一家参与访谈的车企也认为，由于当下与数据安全相关的政策法规密集，面临监管多头问题，企业在合规方面投入了大量时间和精力。

汇量科技认为，一方面，近年来数据领域的法律法规不断发展完善，针对数据出境的监管能够促进行业良性发展，塑造全球竞争力；另一方面对企业合规带来了更大的挑战，企业盈利一定程度上也会受到冲击，相关成本亦随之增加，因此，企业必须密切关注相关政策的变化，以确保数据跨境的合规性。"唯有夯实数据安全和隐私保护的基座，才有底气为全球企业提供安全稳定的产品与服务，连接企业端与用户端。"

问卷调查的结果显示，尽管困难重重，仍有超过半数的企业认为"履行相关数据出境的要求有利于业务开展"。

企业实践难点：

1. 从中国大陆向港澳台地区传输数据的行为，是否属于数据跨境传输？
2. 外资企业没有在境内注册主体，但在境内开展业务或向境内提供产品或服务的，是否属于境内运营？
3. 企业运营的产品仅向境外提供服务，不涉及收集境内的数据，是否属于境内运营？境外主体将直接从境内采集的数据存储在境内服务器，是否属于数据跨境传输？
4. 境外主体访问存储在境内的数据，是否属于数据跨境传输？
5. 境内主体向另一个位于境内的外资企业传输数据，是否属于数据跨境传输？
6. 跨国集团内部传输，是否属于数据跨境传输？
7. 境外员工或人员出差到境内，访问境内的系统或是在境内接收数据，是否属于数据跨境传输？

针对如何识别数据跨境传输行为，请参考上篇问题二中的内容，此处不再赘述。此外，信安标委对数据跨境活动发布的多部国家标准，一定程度上也解释了数据跨境传输场景的识别问题，例如于 2017 年 8 月 25 日发布的《安全评估指南（征求意见稿）》第 3.7 条注释 1 中解释了"数据出境"的具体情形[2]；于 2022 年 12 月发布的《认证规范 V2.0》也通过明确跨国企业在个人信息跨境处理活动中进行认证的主体在一定程度上对数据出境场景进行了划分[3]。

综合上述相关法律法规及国家标准的规定，企业在判断公司业务处理数据的行为是否属于"数据出境"时，需要注意：（1）该等数据是否在"境内运营过程中"收集和产生；以及（2）企业的行为是否属于"向境外提供"，或被境外"访问或调用"的场景。

1. 是否在“境内运营过程中”收集和产生

在判断是否属于"境内运营过程中"收集和产生的数据，应理清"境内"及"境内运营"的含义。对于"境内"的含义，我国目前分为"国境内"和"关境内"两种类型。其中"国境内"指一个国家行使主权的领土范围，其指代范围包括中国大陆、香港特别行政区、澳门特别行政区、台湾地区（以下统称"港澳台地区"）；"关境内"则指使用同一海关法或实行同一关税制度的区域[4]。根据《中华人民共和国出入境管理法》附则中提到的定义，"出境"指由中国内地前往其他国家或地区，包括由中国内地前往香港特别行政区、澳门特别行政区，由中国大陆前往台湾地区。在这种定义下港澳台地区属于"境外"范围。现行法律法规没有明确规定数据处理过程中涉及"境内"的概念，但网信办发布的《网数条例（征求意见稿）》第十三条提出"数据处理者赴香港上市，影响或者可能影响国家安全的"需按有关规定申报网络安全审查。从侧面可以看出国家在数据跨境处理上以保证数据安全为主，对于"境内"的含义也倾向于"关境内"的角度进行解释，即由中国大陆向港澳台地区传输的数据的行为属于"出境"行为。

同时，根据《安全评估指南（征求意见稿）》第 3.7 条注释 1 的规定，向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据，也属于数据出境的情形。由此可以看出对于数据"跨境"的判断，并不拘泥于我们通常理解的数据跨越"关境"边境的传输方式，更着重于强调境外主体是否属于"本国司法管辖"或"境内注册"。其判断标准更偏重"属人原则"而非"属地原则"。**因而，实践中境外员工或人员出差到境内，访问境内系统或在境内接收数据属于数据跨境传输的范围。**

---

[2] 注 1：以下情形属于数据出境：

a) 向本国境内，但不属于本国司法管辖或未在境内注册的主体**提供**个人信息和重要数据；

b) 数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问**查看**的**（公开信息、网页访问除外）**；

c) 网络运营者**集团内部**数据由境内转移至境外，涉及其在境内运营中收集和产生的个人信息和重要数据的。

[3] 认证主体：跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动可由境内一方申请认证，并承担法律责任。《中华人民共和国个人信息保护法》第三条第二款规定的境外个人信息处理者，可由其在境内设置的专门机构或指定代表申请认证，并承担法律责任。

[4] 参考中国社会科学院法学研究所周汉华教授主编的《<个人信息保护法>条文精解与适用指引》，北京：法律出版社，2022，P244。

对于"境内运营"的概念，根据信安标委于 2017 年发布的《安全评估指南（征求意见稿）》中规定，指网络运营者在中国境内开展业务，提供产品或服务的活动。其判断依据不以企业是否在境内注册，而关注企业是否向境内开展业务，或向境内提供产品或服务，包括但不限于以下重点判断因素：

- 是否以为**中国境内居民**提供服务为目的；
- 提供产品和服务的过程中是否使用了**中文**；
- 是否提供了可以用**人民币作为结算货币**的选项；
- 是否提供了**向中国境内配送物流**的服务等。

实践中，如果企业运营的产品仅向境外提供服务，不涉及收集境内的数据；或境内的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务，且不涉及境内公民个人信息和重要数据的，均不视为境内运营。

2. 是否属于跨境传输场景

此外，对于企业实践中涉及的数据出境行为通常分为以下三种类型：

(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

在实践中，可能被认定为数据出境的场景包括：

① 境内运营中收集和产生的数据从境内服务器传输至境外的服务器（如下图 1）

第①种场景通常存在两种传输方式：1）通过具有数据传递功能的软件或硬件等物理介质向境外提供数据；及 2）境内主体通过上传或存储数据至位于海外的服务器或云端。

第一种通过具有数据传递功能的软件或硬件介质向境外提供数据，企业通常能够意识到发生了数据出境，是较容易识别出的场景。其中传递数据的介质可以包括电子邮件、FTP、跨境搭建的 VPN、API 或常见的 U 盘、移动硬盘或便携式笔记本等。第二种数据出境的场景则相对隐蔽，往往被企业所忽视，从而导致违规风险。例如，外资企业的境内子公司使用境外母公司海外部署的数据库作为文档库，上传文档至海外服务器；或员工在境内收集数据后录入、应用收集境内数据后导入部署在境外的客户关系管理（CRM）系统，以实现直接销售、对客户行为和历史的预测和分析、员工访问或调取信息等功能。

② 境内运营中终端（如 App 等应用）采集的数据"直接存储"至境外服务器（如下图 2）

第②种场景则属于《指南（第一版）》中明确规定的数据跨境传输的场景。

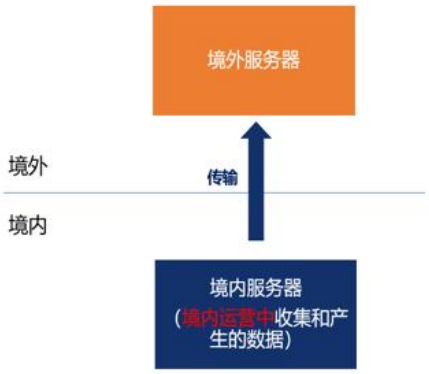


图 1

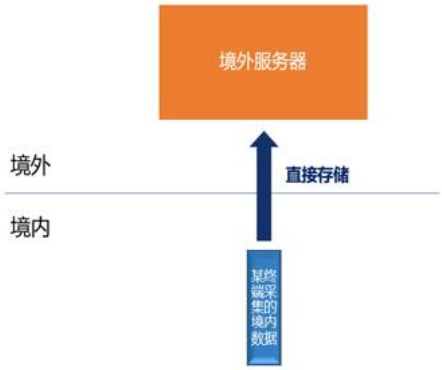
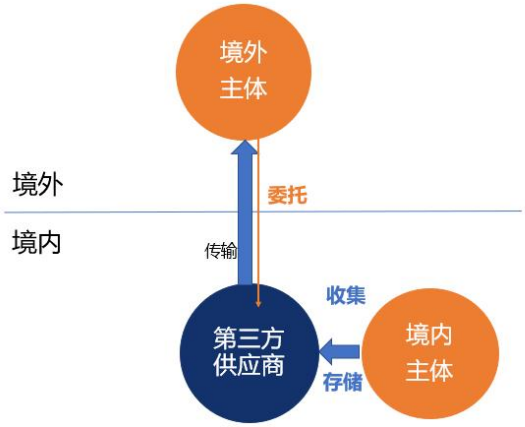
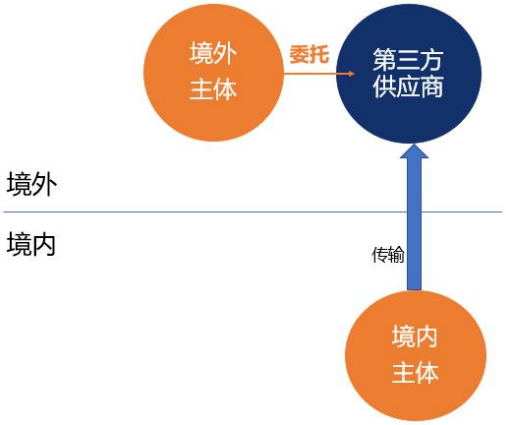


图 2

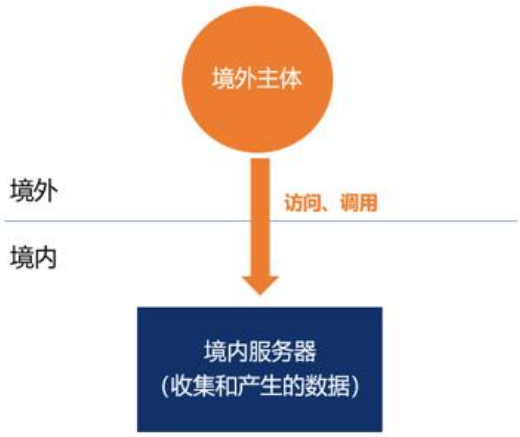
此外，除境内主体和境外主体以外，在数据传输的过程中往往会涉及第三方的情况，例如境外主体委托境内或境外第三方供应商代为收集境内运营中产生的数据（如下图）。在这种情形下，尽管境外主体未直接收集数据，但如果第三方供应商是受境外主体委托而处理数据，则境外主体是数据处理者从而很可能被认定是数据的境外接收方。





（2） 数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用（公开信息、网页访问除外）

评价是否属于数据出境行为时，也应关注重"境外主体获取/访问境内数据"这个因素，即无论境内主体与境外主体如何实施数据传输行为，只要存在于境内运营中产生的数据被境外数据处理者访问、传输、存储（如下图）的情况，则属于数据出境。



由此可见，跨国公司或者同一经济、事业实体下属子公司或关联公司访问或调用存储于境内的数据，属于数据出境。例如，若 FIE 的境外母公司可以访问其存储于中国服务器中的相关数据，该 FIE 也需要依法进行安全评估后方可被其境外母公司访问或者调取。

（3） 境外产生收集的数据在境内存储后再向境外传输

具体来说，境外主体或应用（如 App）将"境外产生收集的数据"（下称"境外数据"）传输至境内，如果境外数据**与境内产生收集的数据"混存"在同一境内服务器上**（尽管进行逻辑隔离），或**在该服务器上对境内外数据进行融合加工分析**，那么当境外主体或应用可访问、调用该境内服务器上的数据（如下图 1）时，此类场景也将被认定为数据出境。

但如境外主体或应用将境外数据传输至境内服务器上，该服务器**仅存储境外数据**，境外主体或应用访问、调用该服务器上的境外数据时，则不属于数据的跨境场景（如下图 2）。《安全评估指南（征求意见稿）》第 3.7 条注释 2 与注释 3，亦将上述场景列明为不属于数据跨境传输的情形：（1）对于非在境内运营中收集和产生的个人信息和重要数据经由中国出境，且未经任何变动或加工处理；或者（2）在境内存储、加工处理后出境但不涉及境内运营中收集和产生的个人信息和重要数据的。

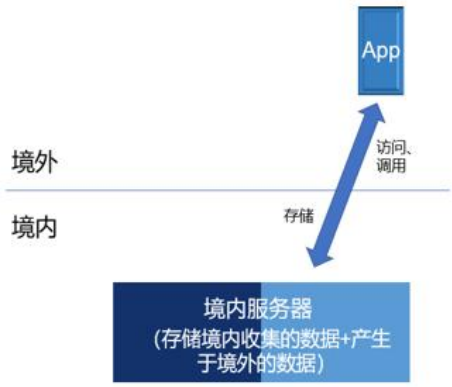


图 1

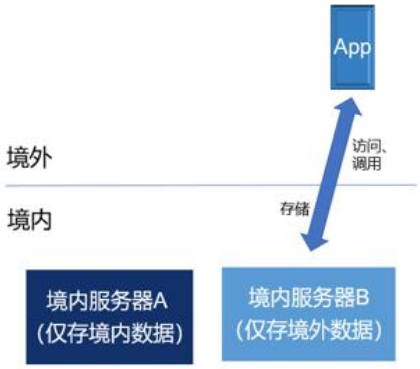


图 2

（4） 其他特殊情形，如境外实体或应用直接收集境内产生的数据。

除上述三种数据跨境传输的情形外，《指南（第一版）》提到数据出境行为还包括"网信办规定的其他数据出境行为"。在实务中比较常见的类型为境外直接收集境内数据。例如，境外公司直接向中国境内用户提供产品或服务，且于境外直接收集境内产生用户数据，在该种情形下，虽然数据的处理行为均在中国境外进行，但其收集的个人信息为向境内提供产品或服务时产生的，符合前述"境内运营"的描述，也属于数据跨境传输的场景。

在实践中，上述跨境传输场景可能发生在境外供应商传输数据至境内企业后，结合境内运营中收集、产生的信息再回传至境外主体。

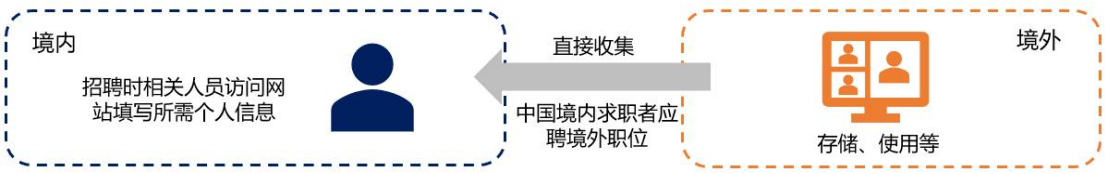
3. 在实践中企业可能涉及的数据跨境传输场景

（1） 人力资源数据出境场景

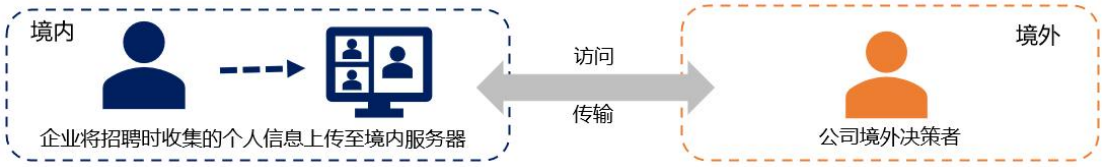
① 公司招聘（应聘者个人信息出境）

在公司招聘的过程中，可能被认定为涉及数据出境的典型场景如下：

- 通过企业网站等方式招聘员工，由应聘人员直接访问境外企业网站填写相关个人信息（如下图）。



- 企业将招聘时收集的境内个人信息上传至境内服务器，随后传输至境外母公司或境外母公司直接访问、调取境内服务器上的数据（如下图）。



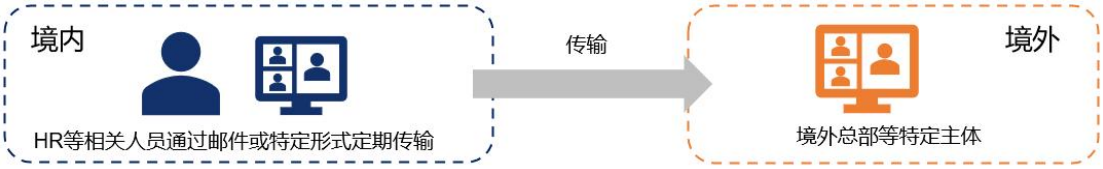
- 企业聘请第三方机构代为招聘员工的场景中，由第三方机构将收集的数据传输至境外（如下图）。

此外，值得注意的是，在招聘过程中由于企业通常收集应聘者的姓名、性别、联系方式、教育程度、工作经验等个人信息用于筛选候选人或准备面试，尚未涉及签署劳动合同，非《个人信息保护法》第十三条规定的（二）为按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的情形。因此，在该种情形下，处理个人信息的合法性基础为告知同意[5]，企业在实践中需注意在招聘过程中获取个人信息主体授权同意或单独同意。

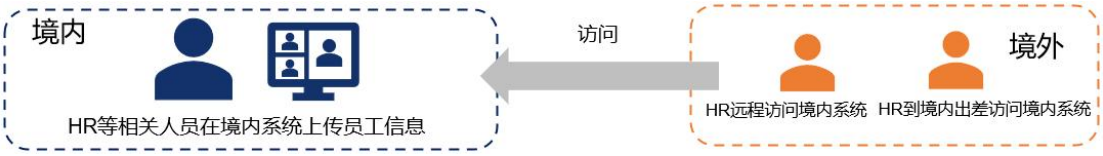
② **员工数据出境**

在公司人力资源管理的过程中，可能被认定为涉及数据出境的典型场景如下：

- HR 等相关人员通过邮件或特定形式定期传输员工数据至境外主体（如下图）；



- HR 等相关人员在境内系统上传员工数据，境外主体于境外远程访问或境外员工出差至境内访问系统（如下图）；



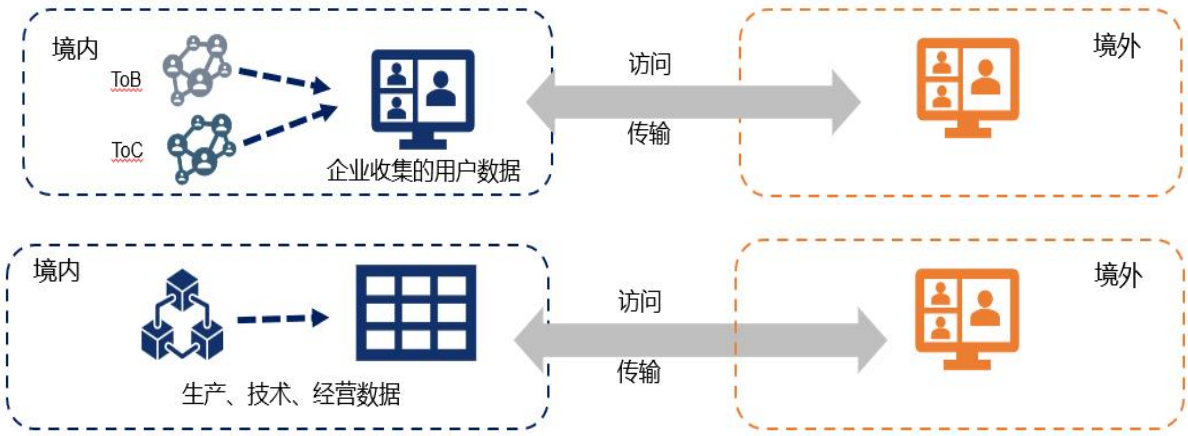
[5] 《个人信息保护法》第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

- 境外通过全球人力资源管理系统直接收集境内员工数据（如下图）

（2） 业务数据出境场景

对于业务数据的出境场景中，可能被认定为涉及数据出境的典型情形如下：

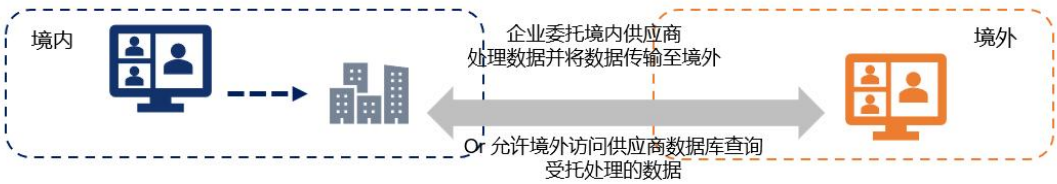
企业收集数据（包括但不限于 To B 和 To C 用户个人信息、生产、技术、经营业务数据（含商业秘密）、重要/核心数据等）并存储至境内服务器中，但可被境外主体或应用访问、调取、下载、导出等（如下图）。



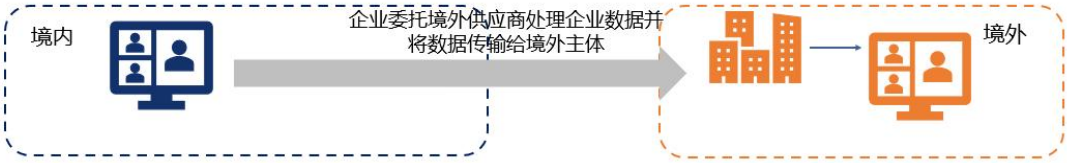
（3） 供应商数据出境场景

在企业委托供应商处理数据的场景中，可能被认定为涉及数据出境的典型场景如下：

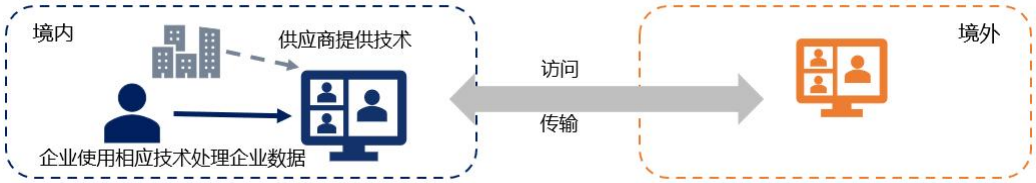
- 企业委托境外供应商处理数据，供应商按照企业委托将数据传输至境外或允许境外主体访问供应商服务器上受托处理的数据（如下图）。



- 企业委托境外供应商处理数据，并将相关数据传输到境外主体（如下图）。



- 企业使用供应商提供的技术或软件将数据传输出境（如下图）。



值得注意的是，在以上场景中，企业均是跨境传输场景中的数据处理者/数据提供方，供应商仅为受托方或技术提供方。

二、 如何准确识别跨境传输数据的类型

重要数据的识别是识别跨境传输数据类型工作中的难点和重点。已在安全领域深耕多年的绿盟科技认为，目前数据出境合规工作中，企业对"重要数据"的定义和范围不够清晰，导致在出境数据自评估时不准确。绿盟科技提出，这种现状需要国家监管及行业主管部门对重要数据做进一步的精细化分类。

一家在海外设有研发机构的车企在访谈中也提到了上述困惑，"由于我们涉及出境的数据主要是双方研发涉及的代码，而代码究竟算不算重要数据，这让我们在日常的工作中感到很困惑，最终只能不确定的都按照最严格的要求来处理。"

深圳数据交易所在近年支撑推动了大湾区地区数据跨境的相关案例实践，其在访谈中也表达了类似观点：由于重要数据的识别标准模糊，一方面，数据处理者因未识别到重要数据，故未履行出境前置程序，但实际上出境数据可能涉及重要数据，存在合规义务未履行的风险。另一方面，部分数据处理者所处理的数据虽安全级别较低，不属于重要数据，但同样由于重要数据识别标准模糊，数据处理者将无需进行安全评估的跨境数据事项向网信部门进行申报，造成了不必要的资源浪费及负担加重。

"对重要数据的划分感到无从下手"是研究团队在访谈中提到次数最多的问题。调查问卷也显示，有近半数受访企业认为"对于重要数据、敏感个人信息等数据类型的标准认定存在模糊，难以做到准确地区分"。有 5 家企业表示虽然跨境数据中包括敏感个人信息，但还未完成对个人信息进行完全的脱敏处理。有 8 家企业没有（或不清楚）识别重要数据的企业标准。

企业实践难点：

1. 如何识别重要数据？产品代码是否是重要数据？
2. 如何识别个人信息及敏感个人信息？
3. 个人信息匿名化处理后是否仍识别为个人信息？
4. 敏感个人信息去标识化处理后是否识别为个人信息？
5. 如果涉及敏感个人信息出境，是否必须去标识化或匿名化处理后才被允许出境？

我国法律法规按照企业属性的不同，针对不同的数据类型的跨境传输提出了不同的要求，具体如下表所示：

关键信息基础设施运营者（CIIO）	一般网络运营者			
个人信息+重要数据	个人信息	重要数据	核心数据	其他数据
因业务需要，确需向境外提供在境内运营中收集和产生的**个人信息**和**重要数据**时，在根据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后方可提供。[6]	向境外提供**个人信息**的，应当向个人告知个人信息的**种类**且征得个人信息主体（或其监护人）的**单独同意**，并满足如下条件之一：（一）通过国家网信部门组织的安全评估；（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；（三）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，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件。[7]	数据处理者向境外提供**重要数据**或**达到一定数量级的个人信息**或**敏感个人信息**，需申报数据出境安全评估[8]；数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估出境数据的种类、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。[9]	有境内存储要求的，应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。[10]	**国家秘密**在对外提供时需要取得相关部门的批准并与对方签订保密协议；**健康医疗大数据**需要进行安全评估审核；**测绘成果**需要按照国务院和中央军事委员会规定的审批程序执行；而**人类遗传资源信息**则需要事先向国务院科学技术主管部门报告并提交信息备份。[11]

[6] 《网络安全法》第三十七条。
[7] 《个人信息保护法》三十八条、第三十九条。
[8] 《数据出境安全评估办法》第四条。
[9] 《数据出境安全评估办法》第四条、第五条。
[10] 《工业和信息化领域数据安全管理办法（试行）》第二十一条。
[11] 具体可参见《中华人民共和国保守国家秘密法》第三十条，《国家健康医疗大数据标准、安全和服务管理办法（试行）》第三十条，《中华人民共和国测绘法》第三十四条，《中华人民共和国生物安全法》第五十七条。

但在实践中，企业往往遇到难以识别个人信息、敏感个人信息、重要数据的问题。

1. 个人信息的识别

《个人信息保护法》与《网络安全法》中均明确了个人信息的概念[12]，其判断的标准主要在于是否**"已识别"或"可识别"自然人个人身份**，而对于匿名化处理过的信息则不属于个人信息的范畴。

需要注意的是，企业通常对个人信息进行去标识化或匿名化处理。从效果上看，对经过匿名化后的个人信息无法再识别到个人，不再是个人信息；而去标识化后的个人信息在借助额外信息的情况下仍可再次识别到个人，仍属于个人信息的范畴。例如企业曾向境外接收方传输用户的手机号码、地址、姓名等完整字段，境外接收方也在其数据库中进行了保留，那么即使本次传输出境方企业使用了去标识化措施，境外接收方仍可以通过撞库或者用户 ID 映射的方式识别到具体个人，此时，离岸后的数据在此场景下依然保留个人信息的属性，应被认为属于个人信息出境。

2. 敏感个人信息的识别

根据《个人信息保护法》，敏感个人信息是指**一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息**，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。相较于个人信息，敏感个人信息遭到损害后会造成更为严重的影响，在跨境传输中的规定也更为严格[13]。《信息安全技术 个人信息安全规范》（GB/T 35273—2020）作为推荐性国家标准，在附录 B 中列举了部分敏感个人信息类型，也对企业合规实践起到了指引的作用。

另外，对于敏感信息去标识化处理后在数据跨境传输中是否仍识别为敏感个人信息的问题，根据咨询网信办等监管部门的结果，如果通过去标识化处理的确能够改变敏感个人信息的性质，使其即使被泄露或者非法使用，也并不会导致自然人的人格尊严受到侵害或者人身、财产安全受到危害，那么**该等处理后的个人信息不属于敏感个人信息**，在评估是否需要进行数据出境安全评估时也不需要再把此类数据纳入"1 万人敏感个人信息"的计算范围内。但是，需要提醒注意的是，由于此类数据仍为个人信息，所以企业仍需要注意其他数据出境安全评估的门槛要求，比如是否总计处理了 100 万人以上个人信息、是否自上年 1 月 1 日起累计向境外提供 10 万人个人信息。同时，监管部门也指出敏感个人信息也可以出境，并非一定要进行去标识化或匿名化处理。

3. 重要数据的识别

---

12 《个人信息保护法》规定，个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息；《网络安全法》规定，个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息。

13 如《数据出境安全评估》中规定累计向境外提供 1 万人敏感个人信息需申报数据出境安全评估，而对于个人信息的数量值则为 10 万人。

现行的法律法规对于重要数据的定义规范的较为模糊，识别重要数据已经成为众多企业在数据出境合规中的"拦路虎"。

在此背景下企业可以从定义、泄露后影响维度和识别要素多方面综合识别重要数据。

从定义上看，根据《数据安全法》第二十一条[14]及《数据出境安全评估办法》第十九条[15]，重要数据指**"一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据"**。目前行业中汽车和基础电信两个领域对重要数据制定了进一步指引，可为企业识别重要数据提供参考[16]。

从数据泄露后可能影响的维度上看，根据《网数条例（征求意见稿）》及《重要数据识别规则（征求意见稿）》，重要数据在篡改、破坏、泄露或者非法获取、非法利用时，会对**"国家政策、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"**等维度产生影响，企业可参考此内容识别重要数据。

从识别要素上看，根据《网数条例（征求意见稿）》及江苏省网信办于 2022 年 9 月 2 日发布的《江苏省数据出境安全评估申报工作指引（第一版）》[17]，可针对**是否属于特定领域[18]、是否涉及特定群体[19]、是否涉及特定区域[20]、是否公开[21]以及是否达到一定精度或规模[22]**等方面进一步识别其是否属于重要数据。例如，对于代码是否属于重要数据的范畴，其需要根据其涉及的行业及泄露后的影响综合判断，若代码中的内容涉及重要行业的信息，如与关键信息基础设施相关的代码，则很可能构成重要数据。

此外，根据《数据安全管理办法（征求意见稿）》第三十八条[23]，重要数据一般不包含个人信息，但个人信息与重要数据仍有交叉的部分，如《网数条例（征求意见稿）》第二十六条[24]规定数据处理者收集 100 万人以上个人信息的，则需遵守处理重要数据的相关法律法规及标准；《汽车数据安全管理若干规定（试行）》规定[25]，重要数

14 第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

15 第十九条 本办法所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

16 具体内容可参见《YD/T 3867-2021 基础电信企业重要数据识别指南》《汽车数据安全管理若干规定（试行）》。

17 具体可参见 http://www.jswx.gov.cn/xinxi/shuzi/202209/t20220902_3068388.shtml。

18 如与出口管制物项、关键信息基础设施相关，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。

19 如与国防科研生产单位相关。

20 如军事管理区。

21 未公开的政务数据、情报数据和执法司法数据属于重要数据。

22 如达到一定规模或精度的基因、地理、矿产、气象数据。

23 第三十八条 重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

24 第二十六条 数据处理者处理一百万人以上个人信息的，还应当遵守本条例第四章对重要数据的处理者作出的规定。

25 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、公共利益或者个人、组织合法权益的数据，包括：（五）涉及个人信息主体超过 10 万人的个人信息；

据包含涉及个人信息主体超过 10 万人的个人信息。两条款虽目前处于试行或征求意见稿阶段，尚未正式生效，但仍对企业合规具有一定指导作用。

实践中，企业可通过对数据全生命周期中数据类型、具体实现方式、涉及相关方等要素的梳理，在全面识别其数据网络中几乎所有数据类型、数量、存储位置、传输流等情况的同时，盘点在实践中处理这些数据的目的和方法，完成以下目标：

- 识别企业涉及的个人信息和重要数据；
- 识别个人信息和重要数据跨境场景及链路；以及评估跨境对个人信息与重要数据影响程度等。

在实践中，企业可以通过人工或与自动化结合的方法，全面识别和盘点各场景下的数据资产，其中包括业务数据、客户数据、配置文件、记录数据（如日志、审计记录）、商务文件（合同、协议等）、技术文档等结构化和非结构化数据。

此外，在数据梳理和识别过程中，信安标委发布并生效于 2021 年 6 月 1 日的《信息安全技术 个人信息安全影响评估指南》（GB/T39335-2020）第 5.3 条提出，在数据映射分析时，除了需要考虑目前数据处理过程中涉及的资源[26]和相关方[27]外，还应当尽可能的考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。对于数据映射的具体形式可参考下表[28]：

数据处理活动/场景/特性或组件	数据类型	数据主体	数据收集、处理目的	数据处理的合法事由	数据处理者	受托数据处理者	是否涉及跨境转移	是否涉及第三方共享
处理活动 A								

三、 如何正确盘点跨境传输数据的数量

《数据出境安全评估办法》第四条规定，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；自上一年 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均应申报数据出境安全评估。

[26] 如内部信息系统。

[27] 如个人信息处理者、平台经营者、外部服务供应商、云服务商等第三方。

[28] 详细内容可参考《信息安全技术 个人信息安全影响评估指南》（GB/T39335-2020）附录 C。

在此背景下，盘点跨境传输数据的数量成为数据跨境合规工作中最基础的一步，也是最困难的工作之一。汇量科技表示，当下很多企业部门众多，数据散落在各个部门中，一旦缺乏统一的管理，想要识别和评估所有数据就难以实现，盘点数据数量更是无从谈起。

调查问卷结果显示，有近七成的受访企业都表示在相关工作中面临着"公司业务和合规要求间存在冲突，难以短时间内调和"的困难，有超过三成的企业存在"对所需履行的申报义务及流程认识不够完整，存在漏报、少报等情况"。

企业实践难点：

1. 达到多少数量级的个人信息需申报数据出境安全评估？
2. 如何统计跨境传输数据的数量？是否需考虑 To B 端处理的数据？
3. 境外访问导致的跨境传输的数据量是否也应算入跨境传输总量中，是否以可访问数据计算？
4. 2022 年 9 月 1 日前已完成数据出境活动是否需要纳入后续申报数量范围？

中国数据领域相关法律法规，根据企业跨境传输的数据类型不同对跨境传输数据的数量作出了不同的限制要求。其中，《个人信息保护法》第四十条[29]在《网络安全法》第三十七条[30]规定 CIIO 的基础上增加了处理个人信息达到"国家网信部门规定数量"的个人信息处理者。对于这两种主体，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。《数据出境安全评估办法》和《网络安全审查办法》等下位法，对于上述"规定数量"做出了细化。

《数据出境安全评估办法》第四条规定，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；自上一年 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均应申报数据出境安全评估。此外，处理个人信息的数量也是影响能否采取签订标准合同的方式作为跨境传输的法律依据的标准之一（具体内容请见《下篇：调查分析篇》"如何评估跨境传输相关法律文件完善程度"部分）。值得注意的是，对于被识别为 CIIO 的数据处理者，不论传输何种数据，均需申报数据出境安全评估31；而对于一般运营主体重要数据的跨境传输，不论传输多少数量级，也均需申报数据出境安全评估[32]。

[29] 第四十条 **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**，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。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；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

[30] 第三十七条 **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；法律、行政法规另有规定的，依照其规定。

[31] 参考《网络安全法》第三十七条。

[32] 参考《数据出境安全评估办法》第四条。

在盘点跨境传输的数据量时，企业可关注以下要点：

1. 在空间维度方面统计数据数量

在空间维度上，统计跨境传输数据的数量时，应全面考虑数据处理流程中所涉及的相关方。例如，除公司收集的用户个人信息外，企业内部员工及客户、供应商等商务联系人的信息均属于个人信息，适用数据出境的一般规则。因此，企业在统计个人信息数量时，尤其在判断是否达到了数据出境安全评估的门槛时，不仅需要计入 C 端用户数量，也应计入内部员工及客户、供应商等 B 端联系人的数量。

此外，统计跨境数据数量时，除境内传输数据至境外这一场景外，境外访问境内运营中收集的数据也属于数据跨境传输场景之一（具体内容请见《下篇：调查分析篇》"如何准确识别数据跨境传输场景"部分），其涉及的数据量也应算入跨境传输总量中。例如，境外员工访问国内数据库以及外籍员工出差到中国访问境内数据库等场景下涉及的数据量也应算入出境数据总量进行评估。根据 2023 年 2 月 13 日咨询监管机构的结果，对于境外数据处理者访问境内数据这一情形的数量应以境外处理者可访问的数据数量计算。例如境内主体在上一年已收集 11 万人个人信息，如境外处理者仅可访问 5000 人个人信息，则出境的数量为 5000 人，无需进行数据出境安全评估；如境外主体可访问境内主体全部，则出境的数据数量为 11 万人，需进行数据出境安全评估。

2. 在时间维度方面统计数据数量

在时间维度上，统计个人信息数量的时间点应为出境时该个人信息传输的数量[33]，即便出境后企业对该信息进行了匿名化处理乃至删除处理，依然不减少已经出境的个人信息数量。如企业自上年 1 月 1 日起已向境外提供超过 1 万人敏感个人信息，即使企业在该等敏感个人信息出境后又进行了匿名化处理，但出境后个人信息的匿名化处理并没有改变其出境时仍为敏感个人信息的事实，仍需要在出境前进行安全评估。

另外，在统计跨境传输数据数量时，除拟进行跨境传输的数据外，还需要统计 2022 年 9 月 1 日《数据出境安全评估办法》生效前已完成出境的数据。对此，浙江网信办在 2022 年 11 月 22 日发布的《浙江省数据出境安全评

[33] 2022 年 11 月 15 日咨询网信办等监管部门的反馈亦得以印证。

估申报工作问答》中进行了进一步的解答，明确表示，对于《数据出境安全评估办法》生效前已完成的数据出境活动无需单独申报，但已出境数据需在此后申报中计入上一年 1 月 1 日后的累计出境数量。因此，如企业在《数据出境安全评估办法》生效前自上一年 1 月 1 日已出境了 9 万人个人信息，即使生效后仅出境 2 万人个人信息，但统计数量为二者相加之和即 11 万人个人信息，达到需申报数据出境安全评估的量级。

四、 如何确认采取哪种出境安全保障机制

对于法律法规中作为出境安全保障机制划分标准的"100 万个人信息"这一数量，有企业提出了不同观点。一家零售行业的互联网企业认为，100 万的数量标准偏低，企业日常业务中很容易达到 100 万。"数据跨境的三种路径出境安全评估、安全认证和标准合同，安全评估覆盖范围过大，其他两种市场化合规路径就没有了空间；而安全评估属于事前许可，非常消耗合规资源"。此外，问卷显示，有"33%的"不确定自己是否需要申报数据跨境安全评估"。

企业实践难点：

1. 在跨境传输数据之前，企业需要进行哪些安全风险评估？
2. 数据跨境传输场景下的个人信息保护影响评估（PIA）、数据出境安全风险自评估、数据出境安全评估是一回事吗？
3. 数据跨境传输有哪些安全保障机制？
4. 如何确认采取哪种安全保障机制？

在跨境传输数据之前，企业需要确认采取一套适合自身情况的流程，依法评估数据出境的安全风险，并采取相应的安全保障机制，这对于数据跨境传输的合规至关重要。

出境合规流程的第一步是企业自行组织评估数据出境的安全风险，包括如下两个步骤：

- **个人信息保护影响评估（PIA）**。根据《个人信息保护法》第五十五条，企业作为个人信息处理者，只要存在"向境外提供个人信息"的处理情况，无论向境外提供个人信息的数量或所涉及的人数，均应进行 PIA。《个人信息保护法》第五十六条规定了 PIA 的内容主要包括：个人信息的处理目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；以及所采取的保护措施是否合法、有效并与风险程度相适应。

实践中，企业可以分四个环节开展 PIA：（1）梳理数据及识别跨境场景[34]；（2）对数据链路进行梳理并分析合规差距；（3）完成合规整改；（4）出具 PIA 报告[35]。

- **数据出境风险自评估。**根据《数据出境安全评估办法》第四条，当企业满足法定条件时[36]，企业需要向网信部门申报数据出境安全评估，而作为申报的前置程序，企业还应当组织开展数据出境风险自评估。（具体内容请见《下篇：调查分析篇》"如何完成数据出境安全评估"部分）。

特别提示企业注意 PIA 与数据出境风险自评估的关系。一般情况下，如果企业拟向境外提供个人信息尚未达到《数据出境安全评估办法》规定的申报门槛，则企业仅需要完成 PIA，并在准备相应的安全保护机制（签订标准合同或进行个人信息保护认证）后即可向境外传输个人信息。但如果企业拟向境外提供的个人信息达到了《数据出境安全评估办法》的申报要求，则企业开展 PIA 的同时还需要进行数据出境风险自评估。由于数据出境风险自评估的范围不仅包括了 PIA 的评估内容，还增加了对境外接收方合规情况、法律环境等评估事项。因此在实践中，PIA 往往可以与针对个人信息的数据出境风险自评估合并完成，企业无需评估两次，而是在 PIA 内容的基础上进一步补充评估，形成《数据出境自评估报告》。但需要注意，PIA 报告和处理情况记录应当至少保存三年，如果企业对于两个自评估合并操作的，则该报告需要保存至少三年。在评估内容上，《个人信息保护法》第五十六条对 PIA 的内容作出了规定，与《数据出境安全评估办法》第五条对数据出境风险自评估的规定相比，数据出境风险自评估的内容在 PIA 的基础上增加了个人信息主体权益维护、出境方和境外接收方是否约定数据安全保护责任义务等内容。而根据《数据出境安全评估办法》第八条，由网信部门开展的数据出境安全评估范围相比于数据出境风险自评估范围更大，不同数据出境风险评估在内容上的差异应引起企业注意。

根据评估情况，企业可进一步确认个人信息出境相应的安全保护机制。《个人信息保护法》第三十八条提出了个人信息跨境传输的三种安全保护机制：（一）通过国家网信部门组织的**出境安全评估**；（二）进行**个人信息保护认证**；（三）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**；（四）法律、行政法规或者国家网信部门规定的其他条件。

---

[34] 实践中，企业往往会同时涉及多个需要进行 PIA 的场景。例如，企业向一位于欧盟地区的数据控制者提供数据，其中包括敏感个人信息，因此不仅涉及"向境外提供个人信息"，还涉及"向其他个人信息处理者提供个人信息"和"处理敏感个人信息"。此时，企业可以将多个需要评估的场景进行合并处理。

[35] PIA 报告和处理情况记录应当保存至少三年。

[36] 《数据出境安全评估办法》第四条：数据处理者向境外提供数据，**有下列情形之一**的，应当申报数据出境安全评估：（一）数据处理者向境外提供重要数据；（二）关键信息基础设施运营者（CIIO）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；（三）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；（四）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。

- **出境安全评估**，网信办发布的《数据出境安全评估办法》已于 2022 年 9 月 1 日生效（（详见本文"（五）如何完成数据出境安全评估"））。

- **个人信息保护认证**，2022 年 12 月 16 日，信安标委发布了《认证规范 V2.0》（详见本文"（九）如何完成个人信息保护认证"）。

- **订立标准合同**，2023 年 2 月 24 日，网信办发布了《标准合同办法》正式稿，将于 2023 年 6 月 1 日起施行（详见本文"（六）如何评估跨境传输相关法律文件完善"）。

《数据出境安全评估办法》《认证规范 V2.0》和近期出台的《标准合同办法》进一步补足、细化《个人信息保护法》第三十八条向境外提供个人信息的保护机制。

然而，在实践中，企业作为数据跨境传输活动中的出境方往往面临难以决策选择何种安全保护机制的难题。

根据《数据出境安全评估办法》第四条，数据处理者向境外提供数据，**有下列情形之一**的，**应当申报数据出境安全评估**：（一）数据处理者向境外提供重要数据；（二）CIIO 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；（三）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；（四）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。而根据《标准合同办法》第四条，**同时符合下列情形**的，可以通过签订标准合同的方式向境外提供个人信息：（一）非 CIIO；（二）处理个人信

息不满 100 万人的；（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。另外，在适用标准合同前，企业还应注意法律、行政法规或者国家网信部门针对出境的具体情形是否还有其他特殊规定。如果没有，则可以采用与境外接收方签署标准合同的措施后，向境外接收方传输个人信息。

比对《数据出境安全评估办法》和《标准合同办法》（同属网信办发布的部门规章）的要求，可以发现，在涉及个人信息出境的情况下，企业如何选择跨境传输安全保护机制需要重点考虑如下四点因素：

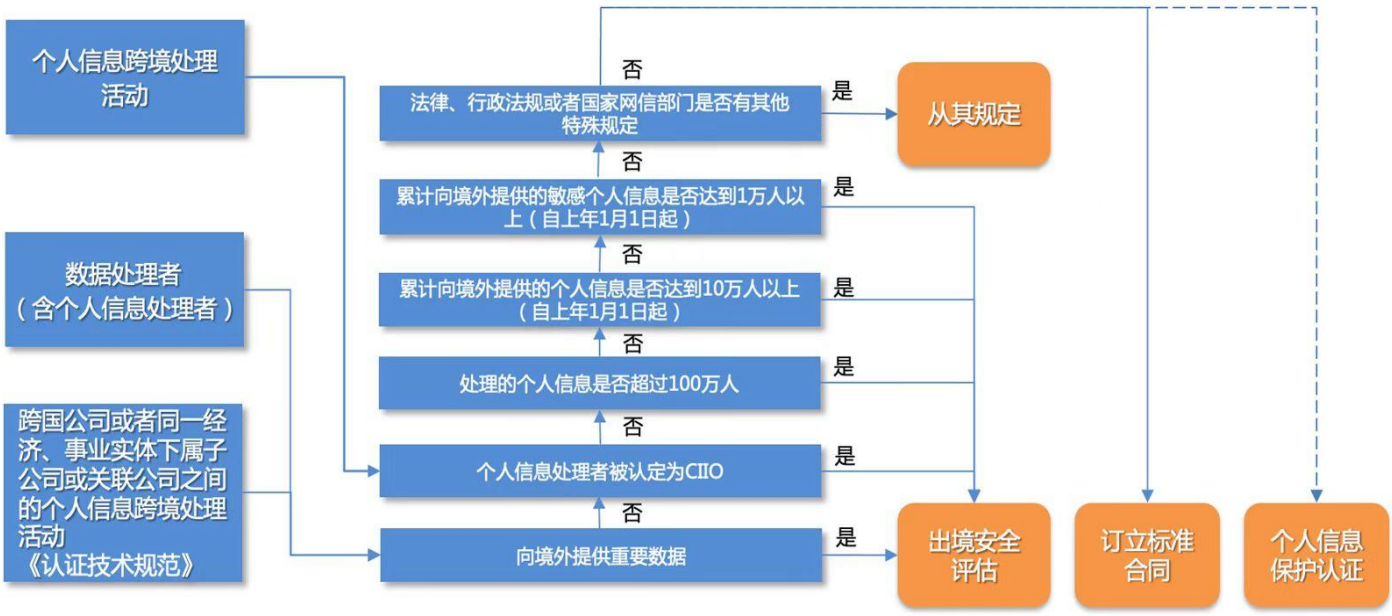
（1）个人信息处理者是否被认定为 CIIO；

（2）处理的个人信息所对应的主体是否超出 100 万人；

（3）累计向境外提供的个人信息所对应的主体是否达到 10 万人以上（自上年 1 月 1 日起）；

（4）累计向境外提供的敏感个人信息对应的主体是否达到 1 万人以上（自上年 1 月 1 日起）。

如果上述四个问题中有一个答案为“是”，则个人信息向境外传输前必须通过申报数据出境安全评估后方能进行，无法仅采用订立标准合同的方式作为个人信息跨境传输的安全保护机制。如果上述问题的答案均为“否”，则在与境外接收方签署标准合同后向境外接收方提供个人信息即可以满足合规要求。虽然《个人信息保护法》第三十八条要求个人信息处理者任选其一方式，但其实在选择顺序上需要先评估是否需要申报出境安全评估，只有当不适用时才能考虑适用出境标准合同或其他机制。另外，值得引起关注的是，如企业存在向境外跨境传输重要数据的情况，则选择申报数据出境安全评估为其唯一安全保护机制。



下文将对上图所示三类安全保护机制做出解读，以便企业更为清晰地了解三者的差异及关系，以及三类安全保护机制的具体要求，在个人信息出境前做出相关准备。

五、 如何完成数据出境安全评估

从问卷调查结果来看，76%的受访企业都进行了数据出境安全评估。但成本高、耗时长和缺乏系统指导是受访企业谈及出境安全评估时最常提及的词语。某大型科技企业在访谈中表示，就其正在经历的出境安全评估来说，省级网信办审查的颗粒度比自己预期高，且更严格，审核周期也比预想的时间长、对报告形式要求也更高。

在跨境数据自评估具有实操申报经验的国科华盾科技有限公司在访谈中表示，很多企业自评估时，由于多元化服务模型中涉及的系统关联关系复杂、处理的数据类型丰富且方法差异大等原因，无法快速、精准、高效的完成自评估申报工作。随着个人数据及重要数据监管的趋严，数据安全领域整体合规难度提高、涉及的评估及整改工作量大、周期长。建议企业特别是涉及数据出境的企业应制定长期目标，提早行动，尽快开始相关评估工作。

企业实践难点：

1. 在达到何种标准时需要申报数据出境安全评估？
2. 如何确定自评估报告出具主体？
3. 如何确认出境接收方？
4. 数据跨境传输合规涉及企业哪些部门，哪个部门适合牵头？
5. 如何按照《数据出境安全评估办法》的要求进行数据出境安全自评估？如何在多系统多场景下高效经济地完成评估工作？
6. 企业申报数据出境安全评估的流程是什么？需要多长时间？如何把握申报时间，什么都还没做的企业选择"躺平"还是"狂彪"？通过数据出境安全评估后，在什么情况下需要再次申请评估？

（一）在达到何种标准时需要申报数据出境安全评估？

具体内容请见《下篇：调查分析篇》"如何确认采取哪种出境安全保障机制"部分，此处不再赘述。

（二） 如何确定自评估报告出具主体？

根据《数据出境安全评估办法》第二条，数据出境安全评估的**申报主体**为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个人信息的数据处理者。对于境外主体直接从中国境内收集重要数据和个人信息、且该主体未在中国境内设立办事机构或分支机构的情况，我们理解也应落在第二条规定的范围之内。即使该境外主体在境内没有分支机构，但因根据《个人信息保护法》第五十三条的规定，以向境内自然人提供产品或者服务为目的或分析、评估境内自然人的行为的境外个人信息处理者应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。因此我们理解数据处理者通过境外直接获取方式如果达到申报标准，也应通过国内指定机构代其进行申报。此外，在实践中，企业通常遇到委托第三方供应商代为处理企业数据的情形。对于该种情形，申报主体需要根据双方签订的协议综合判断—若第三方供应商仅按照企业委托的数据处理目的、数据处理范围内进行数据处理，则属于"代理人"的身份，不属于数据处理者范畴，也不作为数据出境安全申报的主体。

（三）如何识别境外接收方

具体内容请见《上篇：基础问题篇》"如何定义出境数据的境外接收方"部分，此处不再赘述。需要注意的是，在识别到多个境外数据接收方时，需在自评估报告中结合业务场景，根据数据出境规模、涉及国家或地区的风险程度等因素，分别评估各接收方所具备的数据安全保障能力（具体内容请见《下篇：调查分析篇》"如何评估数据处理者和境外接收方的技术和制度措施是否充分"及"如何评估境外接收方法律与政策环境完善程度"部分内容。

（四）如何确定牵头部门

企业在落实数据跨境传输合规措施的过程中，可能会涉及法务、信息安全与安全运维、审计内控、人力资源等多个部门联动。其中，法务部门通常负责识别企业在业务开展过程中的各种数据类型，梳理各种类型数据的传输链路，确定企业与合作伙伴、供应商等各方间的数据处理关系是委托处理还是共享，并安排签署相应的合同或其他法律文件等；信息安全与安全运维部门通常负责制定出境安全操作流程，制定安全管理制度，建立出境数据记录，制定数据出境安全事件应急预案等；审计内控部门通常负责对数据出境安全策略、管理制度、出境操作流程以及对、安全措施的有效性进行审计，妥善保存审计记录，并对审计记录进行定期备份，评估境外接收方所在国家或地区的法律及监管环境等。此外，根据数据出境场景的不同，数据跨境传输合规工作还可能涉及人力资源部门或其他相关业务部门。我们建议企业在开展数据跨境传输合规工作时建立特定部门/团队（实践中为法务部门牵头居多）牵头统筹协调，各相关部门联动配合的工作机制，以法务部门或其聘请的第三方咨询机构对法律法规和标准、指南的解读及相关经验作为合规工作的指引，确保数据出境各环节的合法合规。

（五）如何准备申报数据出境安全评估

2022 年 8 月 31 日，在《数据出境安全评估办法》正式生效实施的前夜，网信办发布《指南（第一版）》，就数据出境安全评估适用范围、申报方式及流程、申报材料、风险自评估、申报咨询方式等具体要求作出了说明。《指南（第一版）》进一步明确了《数据出境安全评估办法》所要求的四份主要材料要求（即申报材料、授权委托书、数据出境安全评估申报书、数据出境风险自评估报告），并补充了其他细化要求。《指南（第一版）》规定，提交表格是"加盖公章的影印件"或"原始文件"，提交方式包括书面材料和电子版材料。此外，《指南（第一版）》要求提交的材料的语言必须是中文。如果只有非中文版本，则必须同时提交准确的中文译本。数据处理者应严格按照《指南（第一版）》准备和提交材料，如提交的材料不够完整，申请将被退回。

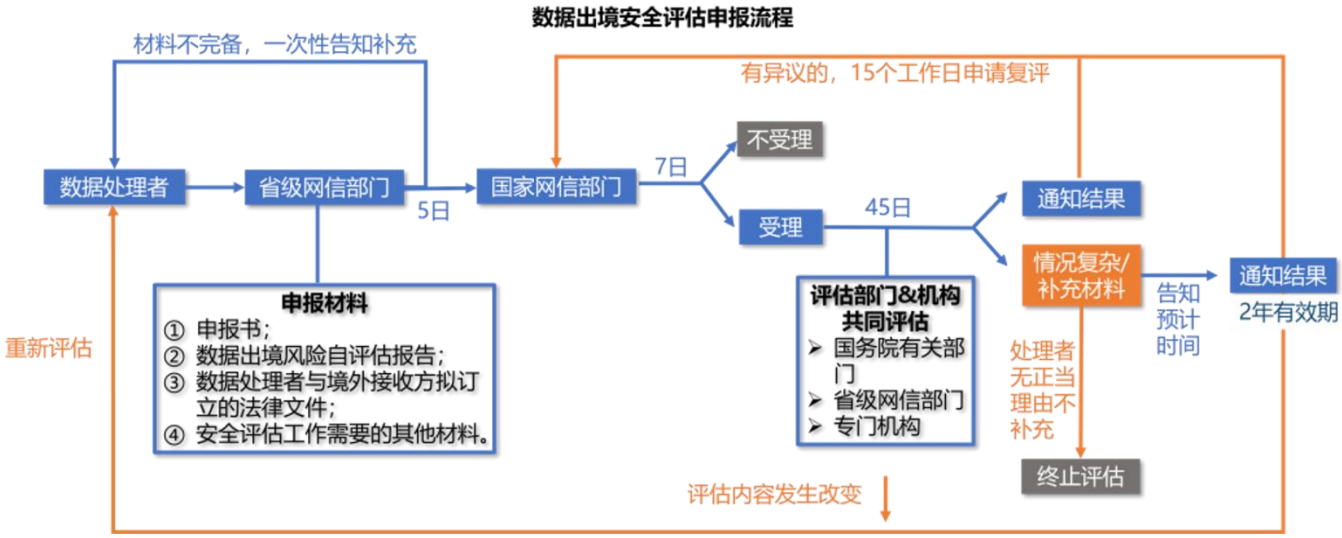
根据《数据出境安全评估办法》的规定，企业在开展数据出境风险自评估时，应重点对数据出境目的的**合法性、正当性和必要性**进行评估。参考《安全评估指南（征求意见稿）》的规定，**合法性**要求出境不属于法律法规明令禁止的，且不属于国家网信部门、公安部门、安全部门等有关部门认定不能出境的情形；**正当性**要求出境已经获得个

人信息主体同意（未经个人信息主体同意但是危及公民生命财产安全等紧急情况除外）；**必要性**要求企业在数据出境活动时需至少满足如下情况之一：1）履行合同义务所必需的；2）同一机构、组织内部开展业务所必需的；3）我国政府部门履行公务所必需的；4）履行我国政府与其他国家和地区、国际组织签署的条约、协议所必需的；5）其他维护网络空间主权和国家安全、经济发展、社会公共利益和保护公民合法利益需要的。我们理解，数据出境目的的合法性、正当性和必要性涵盖了监管部门对数据出境活动应符合法律法规规定、取得（个人信息主体）同意等强制性要求，因此，我们建议企业在数据出境风险自评估工作中，优先对合法性、正当性和必要性进行评估，待确定符合后再开展后续的其他自评估工作。

值得注意的是，企业在实践中，往往遇到难以在多系统多场景下高效经济地完成评估工作的问题，尤其对于境外主体的配合及沟通上有一定的难点。对此，我们建议企业 1）可以先将中国的合规要求及事项传达至境外，在其充分理解评估事项的目的下，由其填写尽职调查清单；2）同时在清单问题的设置上，尽量避免开放式的问题，采取选择题等形式使境外接收方更容易填写清单，减少反馈的时间。

（六）如何把握申报时间

数据出境安全评估预计至少需要 57 个工作日，最多需要 72+N 个工作日（N 代表补充材料审核时间），上述时间均不包括准备材料的时间。数据出境安全评估申请流程如下：



《数据出境安全评估办法》已于 2022 年 9 月 1 日起施行，在施行前已经开展的数据出境活动，不符合《数据出境安全评估办法》规定的，应当自《数据出境安全评估办法》施行之日起 6 个月内完成整改。但应注意的是，虽然《数据出境安全评估办法》规定了 6 个月的宽限期，但是企业在宽限期内如果因数据跨境传输而违反《数据安全法》或《个人信息保护法》时，企业仍有可能承担违法后果。根据《数据出境安全评估办法》第十八条，违反《数据出境安全评估办法》的法律后果以《个人信息保护法》《网络安全法》和《数据安全法》为依据；构成犯罪的，

依法追究相关数据处理者的刑事责任。时至今日，宽限期截止日期（2023 年 3 月 1 日）已至，建议已经提交数据出境安全评估的企业密切关注评估结果[37]；暂未启动申报流程的企业应暂停数据出境活动，待通过出境安全评估后再另行开展，避免在宽限期届满后受到监管关注或处罚。企业可参考上图对申报时间的介绍，结合自身业务情况合理安排申报进度，应尽量选择"狂飙"尽快完成出境安全评估申报工作，以防因行政处罚给企业带来经济损失和声誉上的不良影响。

已通过数据出境安全评估的企业应注意，根据《数据出境安全评估办法》第十四条，数据出境安全评估的结果有效期为自评估结果出具之日起 2 年。在有效期届满后仍需继续开展数据出境活动的，企业应在有效期届满 60 个工作日前重新申报评估。除此之外，如果企业在通过数据出境安全评估后出现向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或延长个人信息和重要数据保存期限的情形，以及《数据出境安全评估办法》第十四条中规定的其他情形，企业应重新申报评估。

我们同时以附件的方式列明了各地网信办数据出境安全评估申报通道，便于企业咨询了解申报工作的相关流程和要求。

六、 如何评估跨境传输相关法律文件完善程度

企业实践难点：

1. 跨境传输数据需要签署哪些法律文件？
2. 跨境传输相关法律文件中有哪些必须约定的事项？
3. 如境外接收方会将出境数据传输给境外第三方，应如何在相关法律文件中约定？
4. 在何种情况下可以适用签署标准合同？
5. 将标准合同作为个人信息出境的安全保护机制，除签署外还应注意什么？
6. 在使用监管机构发布的标准合同时是否可以对内容进行修改？
7. 如果已与境外接收方签署《数据处理协议》（DPA），是否可将标准合同作为其附件？
8. 在《标准合同办法》中存在一些不够精确的表述，应如何理解？

[37] 截至 2023 年 1 月 20 日，北京市申报的首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心合作研究项目（全国首例）和中国国际航空股份有限公司项目已通过数据出境安全评估。参见 https://open.beijing.gov.cn/html//kfdt/sddt/2023/1/1674195507647.html，最后访问于 2023 年 2 月 2 日。

首先，企业需要判断其是否可以适用标准合同作为数据跨境传输机制，从《下篇：调查分析篇》"如何确认采取哪种出境安全保障机制"中的论述中可以看出，相较于出境安全评估，适用订立标准合同的条件更为严苛，需要同时满足四种情形，有任何一种情形不满足，则企业不可以将签署标准合同作为数据跨境传输的安全保护机制，需要借助《个人信息保护法》第三十八条规定的其他传输机制，如完成网信办负责的强制性数据出境安全评估，或从认证机构获得个人信息保护认证。

针对标准合同的内容，网信办于 2023 年 2 月 24 日发布的《标准合同办法》改变了征求意见稿中采用的穷尽式列举的方式，对具体合同内容进一步修订、补充与更新留下转圜余地和灵活操作空间。根据此次公布的《标准合同办法》附件，目前版本的标准合同内容主要包括：（一）个人信息处理者和境外接收方的基本信息，包括但不限于名称、地址、联系人姓名/职务、联系方式；（二）个人信息出境的目的、方式、规模、种类、传输方式、保存期限和地点等；（三）个人信息处理者和境外接收方保护个人信息的义务，以及为防范个人信息出境可能带来安全风险所采取的技术和管理措施等；（四）境外接收方所在国家或者地区的个人信息保护政策法规对合同履行的影响；（五）个人信息主体的权利，以及保障个人信息主体权利的途径和方式；（六）救济、合同解除、违约责任、争议解决等。

由于个人信息出境（跨境传输）是个人信息处理活动的一类，应当遵循《个人信息保护法》对于个人信息处理活动的基本要求，因此《个人信息保护法》对于个人信息处理活动的一般原则也体现在了标准合同模板的部分条款中。具体而言，标准合同主要规定出境方与接收方对于跨境传输个人信息应当履行的义务，未针对双方在数据处理活动中的权利作出明确指引，这些内容可由双方通过其他合同进行补充细化。需要注意的是，根据《标准合同办法》第六条，个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。并且，如果标准合同在达成或订立时与合同双方已存在的任何其他协议发生冲突，标准合同的条款需要优先适用。

目前，我们从实践中了解到，企业在业务开展过程中与境内外实体发生数据交互时，会在专业人士的指导下制定并签署数据处理协议（下称"DPA"）。目前公布的《标准合同办法》并未说明标准合同可以作为主协议附件签署，还是应直接作为主协议签署。企业在签署时应确保双方签署的其他合同（如 DPA）内容不与标准合同文本相冲突。

此外，《标准合同办法》第三条创新地提出了对签署后的标准合同进行的备案要求，相关企业通过订立标准合同的方式作为个人信息出境活动合规措施的，应坚持自主缔约与备案管理相结合的模式。根据《标准合同办法》第六条和第七条，个人信息处理者在标准合同生效后方可开展个人信息出境活动，在标准合同生效之日起 10 个工作日内，个人信息处理者应当向所在地省级网信部门提交标准合同和个人信息保护影响评估报告进行备案。整体流程可以总结为"订立合同→合同生效→开展个人信息出境活动→合同备案"或"订立合同→合同生效→合同备案→开展个人信息出境活动"，可见备案本身并不是标准合同生效的必要条件。另外，《标准合同办法》第八条规定了重新开

展个人信息保护影响评估、补充或者重新订立标准合同并履行备案手续的情形，包括：（一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；（二）境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；（三）可能影响个人信息权益的其他情形。

而当公司需要适用数据出境安全评估作为数据跨境传输机制、无法适用标准合同时，则需要注意评估其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（下称"相关法律文件"）的完善程度。

根据《数据出境安全评估办法》第五条，企业在申报数据出境安全评估前的数据出境风险自评估中，应当对相关法律文件是否充分约定了**数据安全保护责任义务**重点进行评估。同时，根据《数据出境安全评估办法》第八条，企业与境外接收方拟订立的法律文件中是否充分约定了**数据安全保护责任义务**也是数据出境安全评估中重点评估的事项之一。另外，在网信办发布的《指南（第一版）》附件四《数据出境风险自评估报告（模板）》中，"法律文件约定数据安全保护责任义务的情况"也是企业在提交申报数据出境安全评估前必须填写的内容。由此可见，企业在与境外接收方订立合同时，应将传输双方的数据安全保护责任义务作为核心内容进行约定。对于数据安全保护责任义务条款中至少应包括的内容，《数据出境安全评估办法》第九条从数据出境的目的、数据在境外保存地点、对境外接收方将出境数据再转移给其他组织等六方面[38]作出了明确规定，建议企业在起草相关法律文件时应将这些内容涵盖其中。对于相关法律文件中除了数据安全保护责任义务之外的其他内容，企业则可以参考《标准合同办法》中的规定和附件拟订。

此外，在部分业务场景中，如果境外接收方确需将所接收的个人信息再次提供给境外第三方的，在满足向个人告知并取得单独同意等《个人信息保护法》中所列明的条件的同时，建议境内企业在与境外数据接收方所签订的法律文件中以排他性列举的方式明确境内企业所认可的境外第三方（即分处理者或次处理者）。约定未经境内个人信息处理者同意，不得再向境外第三方提供个人信息，并要求境外数据接收方对第三方的过错承担连带责任。

我国数据出境法律不断完善的过程也是出境标准逐渐细化的过程，在监管部门针对相关法律文件出台进一步指导意见之前，建议企业确保相关法律文件内容符合现有法律法规，并按照上述思路分别判断与境外接收方订立相关法律文件是否完善。

---

[38] 第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：
（一）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；
（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；
（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；
（四）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、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；
（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；
（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

七、 如何评估数据处理者和境外接收方的技术和制度措施是否充分

在实践中，对境外数据接收方的考察往往并没有预想的简单。"实际上，我们面对的境外接收方可能就是网店、经销商或者是一个中小企业，规模也比较小，没有安全保障能力，而且它的安全保障能力可没有想象的那么复杂；至于境外的大企业可能就不愿配合，会问'为什么这么多细节？'"一家大型互联网公司在访谈中表示，境外数据接收方的态度和配合意愿也给合规工作带来了不少阻碍。

问卷调查的结果亦显示，目前 77%的受访企业仍主要是靠"在合同中进行约定的方式"来完成判定境外主体履行责任义务的管理和技术措施、能力等保障出境数据的安全，仅有 6 家企业有能力"派遣公司内部人员进行实地考察判断其管理和安全防护能力"，另有 6 家企业"要求对方自行就数据安全、合规进行评估并出具报告"。

企业实践难点：

1. 评估境外接收方数据安全保障能力的范围是否与数据处理者一致？
2. 企业填写的《数据出境风险自评估报告》是否应包含网信办发布的《数据出境风险自评估报告（模板）》中评估数据安全保障能力的全部内容？
3. 实践中，如何与境外接收方沟通，从而对其数据安全保障能力进行评估？
4. 境外接收方无意愿或无能力配合应该如何处理？

《数据出境安全评估办法》第五条提出，数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，其中将境外接收方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列为重点评估事项 。此外，《指南（第一版）》中也将数据处理者及境外接收方的数据安全保障能力作为出境活动整体情况说明的重要部分 。同时，根据 2023 年 2 月 15 日咨询监管机构的结果，企业在填写《数据出境风险自评估报告》时，境外接收方数据安全保障能力的评估范围应与数据处理者一致，不因数据接收方为境外主体而有任何的变化。监管机构的工作人员也表示，在进行材料审查时，也会依据境外接收方的数据管理制度及数据处理的安全技术措施来判断数据出境的风险情况。由此可见，正确评估数据处理者和境外接收方的数据安全保障能力对企业完成数据出境至关重要，而如何正确、充分地评估数据安全保障能力往往是企业在开展数据出境风险自评估时的痛点。

对此，网信办在其发布的《数据出境风险自评估报告（模板）》[39]中列举了评估数据安全保障能力应包含的范围：

[39] 参见《指南（第一版）》附件四的《数据出境风险自评估报告（模板）》。

(1) **数据安全管理能力**，包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况；

(2) **数据安全技术能力**，包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等；

(3) **数据安全保障措施有效性证明**，例如开展的数据安全风险评估、数据安全能力认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评等情况；

(4) **遵守数据和网络安全相关法律法规的情况。**

对于以上评估内容，根据 2023 年 2 月 15 日咨询监管机构[40]的结果，监管机构在进行材料审查时会对企业内部相关制度和数据传输过程中的安全技术进行综合审查，理论上来说上述内容均需要在企业的《数据出境风险自评估报告》中有所体现，并表示企业总结评估的内容越详细，从监管角度上审查时也会认为其数据安全保障能力越强。由此，在实践中，通常分为管理制度保障能力、技术手段保障能力两个方面进行评估：

1. 管理制度保障能力

在管理制度保障能力方面，企业应当根据相关法律法规[41]详细描述数据安全有关的管理组织体系和制度建设情况，例如企业内部的安全管理、人员管理、合同约束、审计机制、应急处理、个人信息权益保护等制度及落实情况[42]。该部分安全保障能力需要法务、安全、技术、审计等部门共同协作评估。

2. 技术手段保障能力

在技术手段保障能力方面，企业应当具备总体安全防护技术手段、数据安全技术防护体系，保障所传输数据的保密性、完整性和可用性。在评估事项中详细描述数据传输时的安全措施，针对数据安全事件的预防、检测及响应能力、数据传输过程中实施身份鉴别和访问控制的能力、保留数据发送日志的能力、对数据发送、传输、销毁等各阶段进行审计的能力以及是否对数据出境传输的安全措施定期评估等[43]。由于该技术部分的评估仅通过制度或用户端的测评无法全部体现，也建议企业在实际自评估时咨询相关领域技术专家的意见，全面充分的评估该方面的保障能力。

---

[40] 北京市网信办。

[41] 包括但不限于《数据安全法》《网数条例（征求意见稿）》《数据出境安全评估办法》《指南（第一版）》。

[42] 可参考阅读孟洁律师团队著《环球评论 | 数据出境合规指引之二——依规开展数据出境安全评估》，https://mp.weixin.qq.com/s/lFBeKQoEDx5bnL4lHGmCAQ

[43] 具体合规义务可参考《数据出境安全评估办法》《指南（第一版）》《数据安全能力成熟度模型》（GB/T 37988-2019）。

同时，企业仍需在《数据出境风险自评估报告》中提供数据安全保障措施有效性证明，例如开展的数据安全风险评估、数据安全能力认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评、ISO 认证等情况[44]，进一步说明其数据安全保障能力。

除此之外，在境外接收方数据安全保障能力的评估方面，根据 2023 年 2 月 15 日咨询监管机构的结果[45]，境外接收方的评估资料应当与境内数据处理者形式和范围保持一致，同时需要保证信息的真实性。在实践中，企业往往担心境外接收方不配合申报工作，难以充分评估境外方的数据安全保障能力。对此，我们建议企业在与境外主体沟通的过程中向其强调**安全评估申报的重要性**，即不完成评估将无法开展数据出境活动[46]；**境外材料的必要性**，即境外材料是评估的重点对象[47]；以及**完成评估时间的紧迫性**，根据《数据出境安全评估办法》第二十条规定，需进行安全评估的企业应在宽限期 6 个月内，即 2023 年 3 月 1 日前完成整改。

八、 如何评估境外接收方法律与政策环境完善程度

在向境外提供个人信息或其他数据前，作为 PIA 及数据出境安全评估的重要组成部分，企业需要评估境外接收方所在国家或区域的法律与政策环境，以判断数据出境活动可能存在的安全风险。

但有企业认为，境外接收方的法律与政策环境相对稳定，由每个企业都独立进行评估可能会带来大量的重复劳动，如果有相关监管部门或第三方机构形成一份成熟的法律与政策环境评估结果，将能够大大增加合规效率，“如果严格按照要求所有目的地都要评估的话，假设跨境贸易如果要和 200 个国家合作，那就要评估 200 个国、地区，这个工作量是非常大的。”

深圳数交所则认为，目前境外接收方的合规义务难核查是一个重要问题。根据现行有效的法律法规等规范文件，对于数据出境链路及数据接收方的数据安全保障能力均有相应的要求，但在实际业务开展中，域外法律识别、政策法规和安全环境评价、接收方数据安全保障能力、数据处理全流程过程等事项核查因为涉及域外核查，开展实地调研及核查存在一定难度及较高成本，企业落实存在一定困难。

---

[44] 具体可参考《指南（第一版）》附件四的《数据出境风险自评估报告（模板）》。

[45] 北京市网信办。

[46] 参见《个人信息保护法》第六十六条、《网络安全法》第六十六条、《数据安全法》第四十六条及《中华人民共和国刑法》第一百一十一条。

[47] 参见《数据出境安全评估办法》第五条。

企业实践难点：

1. 什么时候需要评估境外接收方的法律与政策环境？

2. 应当从哪些角度评估境外接收方法律与政策环境？应当关注哪些要点？

3. 实践中，境外接收方法律与政策环境评估工作应当如何高效开展？

根据《数据出境安全评估办法》《申报指南（第一版）》《标准合同办法》以及《认证规范 V2.0》相关规定，数据出境安全评估的重点评估项包括：

- 境外接收方所在国家或者地区的数据安全保护政策法规和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国法律、行政法规的规定和强制性国家标准的要求；
- 数据安全和个人信息权益是否能够得到充分有效保障，境外接收方所在国家或者地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响。

具体而言，涉及个人信息出境时，境外接收方所在国家或地区的法律政策环境评估主要考虑的要素包括：

（1）该国家或地区现行的个人信息保护法律法规及普遍适用的标准情况，以及与我国个人信息保护相关法律法规、标准情况的差异；

（2）该国家或地区加入的区域或全球性的个人信息保护方面的组织，以及所做出的具有约束力的国际承诺；

（3）该国家或地区落实个人信息保护的机制，如是否具备负责个人信息保护的监督执法机构和相关司法机构等。[48]

[48] 参见《安全评估指南（征求意见稿）》第五条、《标准合同办法》第五条以及《认证规范 V2.0》第 5.4 条 e 项。该三份法律文件均列出了此处三项评估事项。

以“高、中、低”三个等级评判个人信息接收方所在国家或地区的法律政策环境保障能力：[49]

高等级	中等级	低等级
个人信息保护方面的法律法规较为成熟且已形成体系化，广泛使用了标准作为法律法规的补充，保障了个人信息主体的各项权利，有专门个人信息保护机构，同时具备完备、有效、多层次的救济渠道。	个人信息保护方面的法律法规标准基本齐备，保障了个人信息主体的部分权利，有个人信息保护相关负责部门，具备相应的行政、司法救济渠道。	个人信息保护方面的法律法规标准欠缺或不完备，个人仅能通过司法救济渠道维护权利。

涉及重要数据出境时，法律政策环境评估的内容侧重有所不同，主要包括：

（1）该国家或地区在数据安全方面现行的法律法规及普遍适用的标准情况；

（2）该国家或地区主管数据安全的执法机构和相关司法机构等；

（3）该国家或地区的执法机构、司法机构等部门调取数据的权力和法律程序；

（4）该国家或地区与其他国家或地区之间是否缔结有关数据流通、共享等方面的双边或多边协定，包括在执法、监管等方面数据流通、共享的双多边协定。

以“高、中、低”三个等级评判重要数据接收方所在国家或地区的法律政策环境保障能力[50]：

高等级	中等级	低等级
网络安全或数据安全方面的法律法规完备，主管或监管部门具备较强的监督和执法能力，数据安全事件发生后具备有效的追责和监督机制。执法机构和司法机构调取数据的权力受法律的约束，且做到了公开透明，近期不存在相关的负面案例。	网络安全或数据安全方面的法律法规标准基本完备，主管或监管框架初步成型，对数据安全事件主要依靠行政监督，执法机构和司法机构调取数据需要遵循一定的程序。	网络安全或数据安全方面的法律法规标准欠缺或不完备，主管或监管部门不清晰或缺乏相应能力，缺乏在数据安全事件发生后有效追责的机制。执法机构和司法机构调取数据的权力基本不受约束，或近期存在相关的负面案例。

[49] 参见《安全评估指南（征求意见稿）》附录 B.3.3.1。

[50] 参见《安全评估指南（征求意见稿）》附录 B.3.3.2。

对境外接收方所在地法律政策环境的评估也可参考域外的经验。在欧盟法院于 2020 年 7 月作出 Schrems II 案件的判决后[51]，为保证境外接收方可以达到与欧盟同等的个人数据保护水平，欧盟数据保护委员会（EDPB）于同年 11 月发布了《关于补充传输机制以确保遵守欧盟个人数据保护水平的建议》（Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data）及《针对监控措施的关于欧盟重要保障的建议》（Recommendations 02/2020 on the European Essential Guarantees for surveillance measures）[52]，就开展数据跨境传输评估（DTIA）提供指引，尤其强调要评估第三国的数据保护法律或实践。在评估境外接收方所在第三国法律环境时，欧盟数据保护委员会明确了四项"欧盟重要保障"：

（1）数据处理应当基于清晰、明确和公开规则。此处除了评估境外接收方第三国是否具有数据处理的法律基础之外，还应当评估数据保护相关法律规定是否完整明确、是否稳定以及是否具有可预见性；

（2）与合法目标之间的必要性和成比例性。此处特别强调的是，第三国的立法或执法机构基于维护国家或公共安全的目的对个人权利及自由的限制是否必要及适当；

（3）应当具备一个独立、公正的监督机制；

（4）数据主体应当获得有效的救济，包括行使数据主体权利、在权利受到损害时可以寻求司法及其他机构的救济。

综合上述我国及欧盟法律法规的规定，可以总结得出境外接收方所在国家或区域的法律与政策环境的以下评估要点：

（1）法律体系。境外接收方所在地的个人信息保护、网络安全或数据安全的法律法规和标准情况，以及和我国法律体系相比的差异；

[51] 本案中，欧盟法院否定了"美国-欧盟隐私盾"数据传输机制的有效性，因为在此机制下，境外接收方（美国）未能提供与欧盟实质性相同的数据保护水平。

[52] 2021 年 6 月，欧盟委员会更新发布《关于补充传输机制以确保遵守欧盟个人数据保护水平的建议（2.0 版）》（Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0）。

（2）国际承诺。境外接收方所在地加入区域或全球性的数据保护组织、所做出具有拘束力的国际承诺的情况；

（3）落实机制。境外接收方所在地落实个人信息、网络安全或数据安全保护的机制，如：是否具备负责相关的监督执法机构和司法机构、机构的独立性、机构的监督执法能力、数据安全事件发生后是否具有有效的追责和监督机制；

（4）机构权力。境外接收方所在地的执法机构和司法机构等部门调取数据的权力和法律程序，权力是否受到有效的约束、是否能做到公开透明、近期是否存在相关的负面案例；境外接收方是否曾收到其所在地公共机关要求其提供个人信息请求及境外接收方应对的情况[53]；

（5）个人信息主体救济途径。境外接收方所在地是否保障了个人信息主体的各项权利、是否有专门的个人信息保护机构、是否为个人信息主体提供了完备、有效、多层次的救济渠道；

（6）国际协定。境外接收方所在地与其他国家或地区之间是否缔结有关数据流通、共享等方面的双边或多边协定，包括在执法、监管等方面数据流通、共享的双多边协定；

（7）境外接收方所在地在数据方面是否对中国采取歧视性的禁止、限制或其他类似措施等。[54]

在进行评估时，需要获取大量有关境外接收方所在地法律政策环境的信息。

如欧盟数据保护委员会在《关于补充传输机制以确保遵守欧盟个人数据保护水平的建议（2.0 版）》中建议，对第三国当地的法律政策环境进行评估可参考如下信息来源：例如欧盟法院（CJEU）和欧洲人权法院（ECtHR）的判例法；欧盟委员会的充分性认定；政府间组织和区域机构（如欧洲委员会和联合国机构）的决议和报告；该国的判例法或相关独立司法或行政机关作出的决定；独立监督机构或议会机构的报告，商贸、外交、投资机构以及其他相关专业人员制作的报告；学术机构和民间社会组织的报告等。除此之外，也可以参考境外接收方提供的“金丝雀安

[53] 参见《认证规范 V2.0》第 5.4 条 e) 1)项。

[54] 参见蔡开明，阮东辉：《简析〈数据出境安全评估申报指南（第一版）〉》，2022 年 9 月。

全声明（Warrant Canary）”[55]、透明度报告以及其他内部声明或记录，证明境外接收方在足够长的时间内未收到数据访问请求。[56]

由于境外接收方法律政策环境评估工作的专业要求较高，需要评估人员对当地的相关政策、法律、文化、社会等各方面具有充分的理解，因此在具体评估实践中，企业可通过与境外接收方内部法务等相关部门进行合作，或聘请当地律师或其他跨国服务机构协助，以实现全面、深入的评估。

九、 如何完成个人信息保护认证

《个人信息保护法》第三十八条提出个人信息处理者向境外提供个人信息时，需按照国家网信部门的规定经专业机构进行个人信息保护认证。在此基础上，信安标委于 2022 年 12 月 16 日正式发布的《认证规范 V2.0》具体规定了在个人信息跨境处理活动中个人信息保护认证制度的适用情形、认证主体、基本原则、基本要求等内容，为认证机构对个人信息跨境处理活动进行个人信息保护认证提供了认证依据，同时也为企业作为个人信息处理者规范个人信息跨境处理活动提供了参考。

在此次受访的企业中，有 13 家企业进行了“个人信息影响评估”，有 8 家企业进行了“个人信息保护认证”；同时，有 3 家企业涉及相关业务，但并未进行相关评估，5 家企业并未进行“个人信息保护认证”。

企业实践难点：

1. 个人信息保护认证的适用情形是什么？
2. 个人信息保护认证的申请主体有哪些？
3. 个人信息保护认证是否可以替代数据出境安全评估或个人信息出境标准合同，作为个人信息出境的唯一安全保护机制？
4. 企业需要向哪些认证机构申请个人信息保护认证？
5. 个人信息保护认证有哪些具体要求？
6. 个人信息保护认证的具体步骤有哪些？

has not received secret requests for revealing users data to government or law enforcement officers.”

[56] 参见欧盟委员会（EDPB）《关于补充传输机制以确保遵守欧盟个人数据保护水平的建议（2.0 版）》Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, 18 June 2021.

根据《认证规范 V2.0》，个人信息保护认证的**适用情形**为个人信息处理者开展的跨境数据处理活动。作为认证**申请主体**的个人信息处理者应为取得合法的法人资格、正常经营且具有良好的信誉、商誉的境内主体。《认证规范 V2.0》对两类特殊的数据跨境处理活动中申请认证的主体作出了特殊规定，具体如下表所示：

数据跨境处理活动	申请主体（责任主体）
跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动	境内一方
境外个人信息处理者直接收集中国境内的个人信息	境外个人信息处理者在中国境内设置的专门机构或指定代表

在基本原则部分，《认证规范 V2.0》明确了"自愿认证"的原则，即鼓励开展个人信息跨境处理活动的个人信息处理者自愿申请个人信息保护认证，充分发挥认证在加强个人信息保护、提高个人信息跨境处理效率方面的作用。因此，涉及个人信息跨境传输活动的个人信息处理者，是否选择认证完全出于自愿：结合本报告其他三种安全保护机制适用条件的论述，企业在选择是否认证前，需要优先判断是否达到申报出境安全评估的条件，如果达到，则应优先申报出境安全评估。如果企业对自身合规要求基准高且内部预算比较充足，可考虑在申报出境安全评估的同时申请个人信息保护认证，认证为可选项、加分项，出境安全评估为必须项；如果企业未达到申报出境安全评估的条件，且跨境传输的数据涉及个人信息，则企业应当签署出境标准合同并可申请个人信息保护认证（通常亦属于对自身合规要求基准高的企业）；或者只选择申请个人信息保护认证（标准合同与认证二选一）。

对于认证机构的选择，《关于实施个人信息保护认证的公告》与国家市场监督管理总局于 2022 年 6 月 5 日发布的《关于开展数据安全管理认证工作的公告》中并未明确公布依法取得认证机构资质的企业名录。但根据中国网络安全审查技术与认证中心（下称"CCRC"）在其官方网站[57]发布的信息表明，CCRC 负责个人信息保护认证的具体实施工作，且用于办理个人信息保护认证业务的"个人信息保护认证业务管理系统"已经上线[58]。经 2023 年 2 月 2 日向 CCRC 咨询，CCRC 的个人信息保护认证可以涵盖个人信息跨境传输活动，在认证要求、标准上与其他场景存在一定差异。因此，CCRC 可以作为企业对个人信息跨境处理活动申请个人信息保护认证的认证机构。除 CCRC 以外还有哪些认证机构具备认证资格，尚待公布及观察。

《认证规范 V2.0》提出了开展个人信息跨境处理活动的四项基本要求：①个人信息处理者与境外接收方签署具有法律约束力的文件；②开展个人信息跨境处理活动的个人信息处理者和境外接收方均需要既指定个人信息保护负责人，又要设立个人信息保护机构；③与境外接收方约定并共同遵守同一个人信息跨境处理规则，并明确了六项具

[57] https://www.isccc.gov.cn/zxyw/sjaq/grxxbhrz/index.shtml，访问于 2023 年 2 月 2 日。

[58] https://data.isccc.gov.cn/#/pip/login，访问于 2023 年 2 月 2 日。

体内容；④对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。建议企业在申请个人信息保护认证前，按照《认证规范 V2.0》的基本要求，完成合规动作，以顺利通过个人信息跨境处理活动个人信息保护认证。

关于开展个人信息保护认证的步骤，2022 年 11 月 18 日，国家市场监督管理总局和国家互联网信息办公室发布的《关于实施个人信息保护认证的公告》的附件《个人信息保护认证实施规则》，对认证流程进行了进一步细节说明，具体包括认证委托、技术验证、现场审核、认证结果评价和批准等。

十、 如何正确应对国际争议解决场景下取证所涉的数据跨境传输

随着涉及数据跨境的国际诉讼或仲裁案件增多，国内企业特别是小商家面临的合规义务与维权现状引起颇多关注。近来颇受关注的亚马逊商家"封号潮"引起的数据跨境争议便是其中一例。

2021 年 4 月底以来，中国卖家遭遇亚马逊封号潮，约有 600 个中国品牌和 3000 个卖家账号被封。被封账号如要申请回款，亚马逊通知要求必须通过"视频验证"，成功后才有可能回款。但视频验证的正当性和必要性一直饱受广大卖家的质疑，有效同意和告知等程序亦存在不足，验证过程更是涉及到了卖家数据跨境的问题。

目前，要求境外数据接收方依照我国法律法规对合规工作进行配合较为困难，但如果视频验证受阻，国内卖家回款又受到了阻碍，相关方呼吁监管部门能够提供类似申报手册的指引，帮助中国企业在国际争议解决维权案件中保护自身利益，同时也能维护国家数据安全不受影响。

企业实践难点：

1. 为诉讼之目的，向境外司法或执法机构提供存储于境内的数据是否需要向我国监管部门申请审核？
2. 申请审批的部门、流程以及要求提交的材料是什么？

在涉及国际争议解决的场景下，难免会发生要求境内企业向境外司法机构提供存储于境内的数据或个人信息作为证据材料的情况，这便会涉及到数据跨境传输问题。《数据安全法》第三十六条和《个人信息保护法》第四十一条规定，企业向境外司法或者执法机构提供存储于境内的数据或个人信息时，必须经中国主管机关的批准。2022 年 6 月 24 日，司法部在《国际民商事司法协助常见问题解答》中强调，涉及到国际司法协助的，非经中国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中国境内的数据或个人信息。

不论是境内企业提供或外国司法机构调取，均应当提前向中国相关主管机关提出申请，相关主管机关将依据有关法律、中国缔结或参与的国际条约和协定或者平等互惠原则来处理其关于提供存储于境内数据或个人信息的请求。具体来讲：

在国际刑事领域，国家监察委员会、最高人民法院、最高人民检察院、公安部、国家安全部等部门是开展刑事司法协助的主管机关。涉及国际刑事的司法协助将由以上部门依据《中华人民共和国国际刑事协助法》等法律及相关国际条约和协定进行处理。

在国际民商事领域，司法部是开展民商事司法协助的主管机关。涉及民商事领域的司法协助将由司法部根据《海牙送达公约》《海牙取证公约》以及目前缔结的 38 项中外双边司法协助条约规定途径，以及外交途径开展。

实践中，较为常见是企业涉及在境外的民事诉讼纠纷，需要将有关数据信息作为证据材料提交给外国法院或其他司法机构。根据 2022 年 10 月司法部司法协助中心对于相关咨询问题的答复，无论是企业主动向境外司法机构提供证据还是企业应境外司法机构的要求被动提交证据，企业均需要向司法部提供特定材料申请审核。一般情况下所需提交的材料包括：

（1）申请书，应说明外国法院所涉案件的基本情况，外国法院对证据提交的要求（法院命令、对方当事人动议）等信息；

（2）证据清单，应对拟提交的证据材料进行详细说明，包括证据名称、证明事项、与案件的关联性、是否涉及国家安全、国家秘密、政府相关文件、商业秘密、个人信息等；

（3）自评估报告，即企业对拟提交证据材料的初步审核意见；

（4）法律评估报告，即企业法务部门或律师事务所对拟提交证据材料的法律意见。

司法部司法协助中心在收到上述材料后，将会同最高人民法院、网信办、申请企业的业务主管部门（如工信部）等对拟出境的证据进行审核。审核时限通常为 1 个月，涉及重大复杂的案件则为 2 个月。审核通过后，将会为申请企业出具批文，申请企业可以办理出境事宜。目前，在《个人信息保护法》和《数据安全法》生效后已经有不少企业根据上述流程向司法部提交审核申请并得到了批准。

此外，随着中国对于数据安全的保护力度不断增强，相关主管机关也在不断提高当事人申请的便捷程度与相关部门的审核效率。如上文所述，涉及司法诉讼方面的数据出境将以司法部意见为准，将由司法部组织其他有关部门针对企业提交的材料进行会签，企业或无需再向网信部门进行申报。相比于企业自行分别联系网信部门、业务主管部门等申请评估，这将有助于节省企业的成本、提高数据作为证据出境的效率。

综上，我们建议企业在涉及国际争议解决场景时，应当主动与司法部进行沟通，尽早了解相关流程以及所需提交的材料，并按要求申请审批。防止因未能正确预估司法部等相关部门审核的时间及成功率，导致无法按时提交证据的情况发送，增加败诉风险。

同时，值得关注的是，在司法协助的场景下，受到出境限制的并不仅限于重要数据或个人信息，而包括存储于境内的所有类型的数据。即使企业认为拟出境的证据材料中不涉及重要数据及个人信息，或者当企业无法确定证据中所包含的数据类型时，均应提交司法部审核。企业无需将审核流程视为一种"麻烦"，而应将其视为一种对于企业自身合法权益及国家安全利益的司法保护。

附件：各地网信办数据出境安全评估申报通道

地区	联系电话	联系邮箱	链接
北京	010-67676912	/	https://mp.weixin.qq.com/s/qt3X4O35a7fFfKbaHDO6Fw
江苏	025-63090194 025-86292793	yuzhou@jscert.org.cn	https://mp.weixin.qq.com/s/CrxTrqE1kfrQTB99Wte41w
天津	022-88355322	/	https://mp.weixin.qq.com/s/BTCHplCt9kEtZeVM4sK7og
河北	0311-87909716	jscs@caheb.gov.cn	https://mp.weixin.qq.com/s/p6aKaGQ-dTFCtfMmJ0zdlA
浙江	0571-81051250	data_sec.zjwxb@zj.gov.cn	https://mp.weixin.qq.com/s/oZgPppH9VpIwzbxBe0hXJw
上海	64743030-2711	/	https://mp.weixin.qq.com/s/GovsOkRtlEZh0D5Uz1L2ew
福建	0591-86300613	/	https://mp.weixin.qq.com/s/cRcJeVLiiVHp4mqV1fF6kA
内蒙古	0471-4821277	sj_nmgwxb@nmww.gov.cn	https://mp.weixin.qq.com/s/Fb5q7SUZK1XGEkzDoMUzXA
重庆	023-63151805	/	https://mp.weixin.qq.com/s/ZZ5KkiSGU6GRPeX8js-z0g
贵州	0851-82995001	gzcert@cert.org.cn	https://mp.weixin.qq.com/s/9ibgoBflvocewv7ORDgq4w
山东	18853135773 0531-51773249 0531-81913920	/	https://mp.weixin.qq.com/s/obdIRDbYWUBtTmkSO0z33w
海南	0898-65314756 0898-65334103	swwxbxxh@hainan.gov.cn	https://mp.weixin.qq.com/s/uZHQHb6ytfTIcTW3lOoW4g
广东	020-87197742	/	https://mp.weixin.qq.com/s/hQ2Q7LrDRPcl2eoz_hT-kA
山西	0351-5236020		https://mp.weixin.qq.com/s/NNLGyjViPfzYXVdLdhw24A
江西	0791-88912242	swwxbappjb@jiangxi.gov.cn	https://mp.weixin.qq.com/s/dCXAX-pflgeRttS8qGOWpA
云南	0871-63902424	sjcj@yncac.gov.cn	https://mp.weixin.qq.com/s/KYF5NLJleEnZy56jW02wIQ
湖北	027—87796799 027—87231397	/	https://mp.weixin.qq.com/s/Bif2J5SoZjhOvHgzwb2NUg
宁夏	0951-6668922	/	https://mp.weixin.qq.com/s/BjSaauJ-xGoROzs-9e8-2A
辽宁	024-81680082	/	https://mp.weixin.qq.com/s/LF9xVXaOVn_m9kycxOXlbg
四川	028-86601862	/	https://mp.weixin.qq.com/s/OVplosxPzmtdPKwTO788Mg

报告出品：斑马数据合规研究中心

报告撰写：环球律师事务所 孟洁 戴畅 王程 张楚淇 李晨瑜 田梓仪

南财合规科技研究院 吴立洋 王俊 张雅婷 尤一炜 郑雪 谭砚文

设计统筹：林军明

封面/排版：林潢 陈国丽

校对：黄志明

联系方式：E. mengjie@glo.com.cn