NIO蔚来　奇安信　Ogilvy　YOUZAN

环球律师事务所
GLOBAL LAW OFFICE

威科 Wolters Kluwer

数据出境合规实务

50问（2024版）

2024年12月

前言

随着数字经济的蓬勃发展，数据已经成为重要的生产要素和关键的发展引擎。数据跨境流动是充分释放数据红利、打造新发展格局战略支点的重要路径，正在对全球经济发展、科技创新和国际贸易等方面产生愈发深远的影响。然而，数据跨境流动也伴随着数据安全、隐私保护等方面的挑战和争议，因此，各国纷纷加强数据跨境流动的监管和规范。

我国已出台的《数据出境安全评估办法》等法律法规，虽初步搭建出数据出境合规监管框架，但由于细则规定不够明确，企业在数据出境时往往需要结合其主体类型、出境数据类型和累计出境的数量等，综合判断采取何种数据出境制度（即“申报并通过数据出境安全评估、签署并备案个人信息出境标准合同（简称“SCC”）、获得个人信息保护认证”的统称）。自 2023 年 9 月 28 日，国家网信办发布《规范和促进数据跨境流动规定（征求意见稿）》之日起，社会各界便对数据出境合规措施的选择展开了广泛讨论。

历经半年，国家网信办对各方提出的反馈意见进行了细致研判，于 2024 年 3 月 22 日正式公布了《促进和规范数据跨境流动规定》（简称“《规定》”），该《规定》自颁布之日起施行。《规定》对数据出境监管框架进行了细化，进一步放宽了数据跨境流动条件，且相对收窄了数据出境安全评估范围，把“促进”调整到了“规范”前面，释放出要确保在保障数据安全的前提下，更加关切国家经济发展，通过便利数据跨境流动，降低企业合规成本，促进服务贸易与数字经济的大力开展和实施。

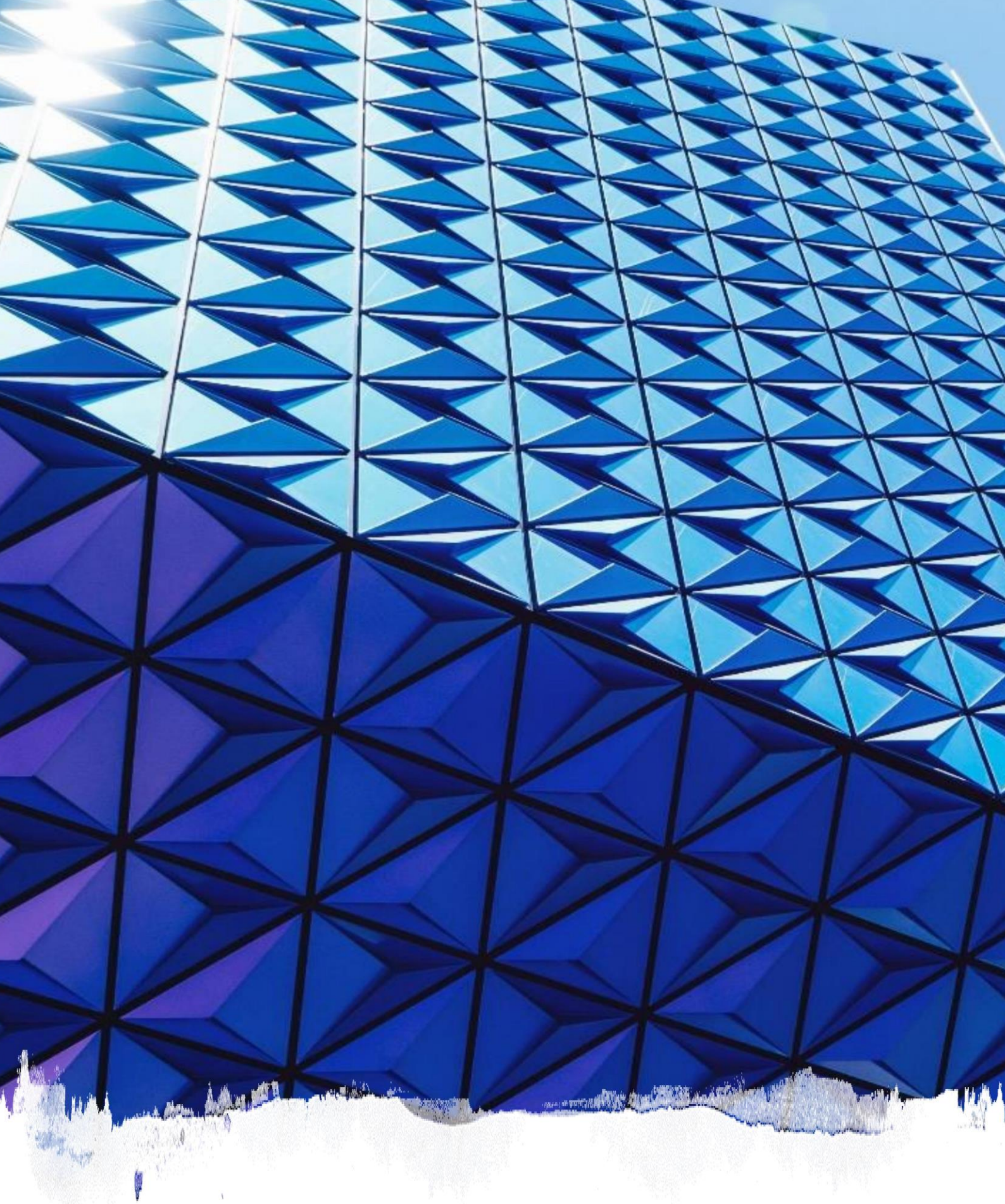
因《规定》对企业选择数据出境制度会产生重大影响，环球律师事务所数据团队联合对外经济贸易大学数字经济与法律创新研究中心、蔚来控股有限公司、奇安信科技集团有限公司、北京奥美互动咨询有限公司、杭州有赞科技有限公司发布《数据出境合规实务 50 问》（2024 版）（以下简称“《实务问答》”），旨在结合业务实践需求，通过分析加问答的形式来解答企业关切的数据跨境传输重点问题。《实务问答》分为上下两篇，上篇为基础篇，主要介绍了数据跨境传输的法律法规框架、相关概念及注意事项辨析等；下篇为实践篇，详细阐述

了数据跨境传输场景的识别、数据类型的确定、数据出境安全评估申报的流程以及风险评估与应对措施等。

在数字经济快速发展的时代背景下，数据跨境传输的合规管理将成为企业不可或缺的重要能力。我们希望通过本《实务问答》的发布为企业提供有益的参考和借鉴，共同推动数据跨境传输的规范发展，为构建安全、高效、有序的数字经济环境贡献力量。

最后，感谢所有参编单位及人员的辛勤付出，特别感谢威科先行的大力支持，感谢各位老师提供的宝贵意见和建议。

目 录



上篇：基础篇

一、 我国有哪些数据跨境相关的法律法规要求？

随着经济全球化和数字化的深入发展，数据跨境传输已经成为全球经济的关键推动力。跨境数据在国际贸易活动、跨国科技合作、数据资源共享方面发挥越来越重要的作用，数据跨境流动已经成为推动数字经济发展，保障全球互联互通的重要途径。

我国对数据跨境流动的规制起步较晚，对于数据跨境传输的限制与监管规定散见于各类法律法规、部门规章以及规范性文件中，处于持续创新和完善、趋向成熟体系形成的过程。

数据出境的法律渊源可以追溯到 2017 年 6 月 1 日实施的《中华人民共和国网络安全法》（下称**《网络安全法》**）。《网络安全法》首次提出了数据出境的安全评估制度，要求关键信息基础设施运营者（下称 **CIIO**）因业务需要向境外提供个人信息和重要数据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[1]。随后，全国网络安全标准化技术委员会（TC260）（下称**网安标委**）于 2017 年 8 月 30 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）》**），在《数据出境安全评估办法》未发布前对数据出境安全评估流程、评估要点以及评估方法等内容提供指引。

2021 年 9 月 1 日实施的《中华人民共和国数据安全法》（下称**《数据安全法》**）重申了 CIIO 跨境传输在境内运营中收集和产生的重要数据需进行评估的要求，并为出台其他数据处理者的重要数据出境监管制度提供了原则性规定[2]。此外，《数据安全法》对向境外司法和执法机构提供数据作出了限制，要求境内组织、个人向外国司法或者执法机构提供存储于中华人民共和国境内的数据必须获得主管机关批准[3]，这也与随后颁布的《中华人民共和国个人信息保护法》（下称**《个人信息保护法》**）提出的“非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息”的要求相呼应。

[1] 《网络安全法》第三十七条。
[2] 《数据安全法》第三十一条。
[3] 《数据安全法》第三十六条。

2021 年 11 月 1 日，《个人信息保护法》施行。同月，国家互联网信息办公室（下称**国家网信办**）发布了《网络数据安全管理条例（征求意见稿）》（下称**《网安条例（征）》**），设专章对“数据跨境安全管理”作出具体规定[4]。《个人信息保护法》第三十八条和《网安条例（征）》第三十五条列明了数据出境应采取的三条主要合规路径，即“通过网信部门组织的安全评估”、“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”、“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”（以下合称**数据出境制度**）[5]。

随后，为推动上述数据出境制度落地，国家网信办及相关行业主管监管部门陆续出台了一系列政策文件。

对于“个人信息保护认证”，国家市场监督管理总局和国家网信办于 2022 年 11 月 4 日联合发布《关于实施个人信息保护认证的公告》（下称**《认证公告》**）及附件《个人信息保护认证实施规则》（下称**《认证规则》**），规定了开展个人信息保护认证的基本规则，标志着我国个人信息保护认证制度的正式建立。网安标委于 2022 年 6 月发布的《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》（下称**《认证规范 V1.0》**）进一步为“个人信息保护认证制度”提供了落地支撑。随后，网安标委又于 2022 年 12 月发布了《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》**），从具有法律约束力的协议应明确的内容、个人信息保护机构应承担的职责、个人信息保护影响评估应涵盖的事项、个人信息主体应享有的权利以及个人信息处理者和境外接收方应承担的责任义务等五方面对《认证规范 V1.0》进行了细化。2023 年 3 月 16 日，网安标委发布了国家标准《信息安全技术 个人信息跨境传输认证要求（征求意见稿）》（下称**《跨境认证要求（征）》**），为推荐性国家标准，在效力层级上高于《认证规范 V2.0》。《跨境认证要求（征）》除增加“敏感个人信息”和“单独同意”的定义并删除了“认证主体”的相关要求外，整体内容与《认证规范 V2.0》基本一致。2023 年 11 月 1 日，网安标委依据《关于促进粤港澳大湾区数据跨境流动的合作备忘录》和属地相关法律法规，制定了

[4] 《网安条例（征）》第五章。
[5] 《个人信息保护法》第三十八条。

《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》，规定了粤港澳大湾区跨境处理个人信息应遵循的基本原则和保护要求，为粤港澳大湾区个人信息保护认证的实施提供了认证依据。

对于“数据出境安全评估”，国家网信办于2022年7月7日发布《数据出境安全评估办法》（下称**《评估办法》**），自2022年9月1日起施行，规定了数据出境安全评估申报的具体情形以及要求；对于“个人信息出境标准合同”，国家网信办则于2023年2月22日发布《个人信息出境标准合同办法》（下称**《标准合同办法》**），自2023年6月1日施行，规定了可以选择签署并备案标准合同的情形，并提供了标准合同范本。

在数据出境制度下的三条合规路径已经初步成型的基础上，为优化完善数据出境制度，实现与数据出境安全风险的“精细化匹配”，并同时促进和规范数据依法有序自由流动，国家网信办结合迄今数据出境安全管理工作的实践情况，于2024年3月22日发布了重量级文件《促进和规范数据跨境流动规定》（下称**《跨境流动规定》**）。

《跨境流动规定》主要从五方面对数据出境制度进行了优化：首先，明确了重要数据的认定标准；其次，提出了免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件；第三，设立了自由贸易试验区负面清单制度；第四，对需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动门槛标准进行调整，适当放宽数据跨境流动条件，适度收窄数据出境安全评估范围；第五，延长了数据出境安全评估结果的有效期限。

同时，为了配合《跨境流动规定》落地，国家网信办于同日发布了《数据出境安全评估申报指南（第二版）》（下称**《评估申报指南（第二版）》**）和《个人信息出境标准合同备案指南（第二版）》（下称**《标准合同备案指南（第二版）》**），对申报数据出境安全评估、备案个人信息出境标准合同的方式、流程和材料等具体要求作出了说明，对数据处理者需要提交的相关材料进行了优化简化。

《跨境流动规定》《评估申报指南（第二版）》《标准合同备案指南（第二

版)》的出台反映了主管部门对数据出境治理思路的变化，即在保障数据“依法有序流动”从而为组织或者个人跨境业务合作提供法治保障的同时，促进数据“自由流动”并进一步推动数据自由流动和数字经济发展。一方面，明确监管部门强化事前事中事后全领域的监管，加强指导监督向境外提供数据的数据处理者履行义务的情况，如告知、取得个人单独同意、进行个人信息保护影响评估、采取技术措施保障数据安全出境以及向省级以上网信部门和其他有关主管部门报告数据出境安全事件等。但另一方面，通过畅通数据跨境传输制度渠道打造跨境数字贸易新格局，鼓励企业积极开展数据跨境流动并推进国际贸易发展，如针对不同商业活动场景需求，在不包含个人信息或者重要数据的前提下，允许国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中产生的数据出境活动不适用数据出境安全评估、个人信息出境标准合同和个人信息保护认证机制，极大地减轻相关企业的合规成本。

《跨境流动规定》的发布标志着企业迎来了全新的数据跨境合规窗口期。该规定不仅提升了现行数据出境制度的实用性和可操作性，还积极回应了企业数据跨境传输业务合规方面的常见困惑，从而降低了企业在数据出境活动中所面临的业务合规挑战和难度。对此，涉及跨境传输数据的企业应把握窗口期时机，依法梳理自身数据出境的场景以及对应合规操作要点，确保在积极参与国际经营和跨境业务合作的过程中不触及数据监管红线。

继国家网信办发布《网数条例（征）》近3年后，2024年8月30日，国务院第40次常务会议通过了《网络数据安全管理条例》（以下简称“《网数条例》”），2024年9月24日《网数条例》正式发布并将于2025年1月1日开始施行。《网数条例》第五章规定了涉及数据跨境传输的安全管理要求，重点包括如下方面：

1. 向境外提供个人信息的合规机制

在总结《评估办法》《标准合同办法》《跨境流动规定》等部门规章制定实施经验基础上，《网数条例》进一步明确了国家网信部门在网络数据出境活动中的功能与作用，同时优化了我国数据出境制度。《网数条例》第三十五条规定了七种向境外提供个人信息的条件以及一项兜底条款，既融合了三条主要合规路

径，也包括《跨境流动规定》中规定的豁免情形；并且，结合《网数条例》第三十六条规定的依据中国加入的国际条约、协定向境外提供个人信息的特殊情形，目前，我国合规地向境外传输个人信息的条件总共有以下八项：

1)通过数据出境安全评估：通过国家网信部门组织的数据出境安全评估；

2)取得个人信息保护认证：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；

3)签订个人信息出境标准合同：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；

4)履行合同所必需：为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；

5)人力资源管理所必需：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跨境人力资源管理，确需向境外提供员工个人信息；

6)履行法定义务所必需：为履行法定职责或者法定义务，确需向境外提供个人信息；

7)紧急情况：紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息;

8)法律、行政法规或者国家网信部门规定的其他条件。

9)国际条约规定：中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

2. 向境外提供重要数据的合规机制

《网数条例》第三十七条基于《评估办法》的规定，要求网络数据处理者在中华人民共和国境内运营中收集和产生的重要数据确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。

关于重要数据的认定标准，《网数条例》在此重申了二点：其一，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需要具有十足的必要性，故相关企业需要自行评估论证，并提供相关证明材料以支撑“确需”提供之说；

其二，根据《跨境流动规定》的要求，重要数据的认定以地方和行业主管部门的通知或公开发布为标准。若相关企业未被相关部门、地区通知处理了重要数据，或者相关部门、地区公开发布的重要数据目录清单中暂未包括本企业所处理的数据的，则企业无需将某类数据作为重要数据申报数据出境安全评估[6]。

3. 向境外提供数据时的其他合规义务

在《评估办法》对于数据出境安全评估内容要求的基础上，《网数条例》第三十八条明确提出，网络数据处理者通过数据出境安全评估后向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。因此，企业在通过数据出境安全评估后，应当严格按照评估材料以及与境外接收方合同约定的内容开展数据跨境传输活动。如果实际的跨境传输活动超过评估时申报的内容，则企业可能被国家网信部门认定为“数据出境活动在实际处理过程中不再符合数据出境的安全管理要求”，因此国家网信部门可能会依据《评估办法》，要求企业终止数据出境活动；如企业需要继续开展的，则应当按照要求整改后重新申请评估。

此外，《网数条例》第三十九条一再强调了数据跨境传输过程中，网络数据处理者对安全风险的防范责任。从具体实施的角度，既包括国家将采取措施，防范、处置网络数据跨境安全风险和威胁，也包括任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等，以此遏制黑客等组织在社会上扩散犯罪工具；也不得在明知他人从事破坏、避开技术措施等活动，仍为其提供技术支持或者帮助。本条明确，即使个人或组织本身没有直接参与破坏、规避技术措施，只要存在上述行为，同样需要承担法律责任，以此有效减少“共犯”行为，进一步遏制犯罪发生。

[6] 目前，我国各地区正在积极探索建立数据分级分类保护制度，制定数据跨境流动的正面/负面清单，明确“重要数据”的类型。例如，天津自由贸易试验区于今年 2 月 5 日率先发布了《中国（天津）自由贸易试验区企业数据分类分级标准规范》将数据分为 13 大类 40 子类，核心、重要、一般三个级别；上海临港新片区于今年 2 月 8 日发布《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》，提出对跨境数据进行分类分级管理，并提出重要数据目录制定、应用与更新机制的管理要求；北京市网信办等三部门也于 8 月 26 日印发《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》，首批选择汽车、医药、零售、民航、人工智能等 5 个领域率先制定，详细列明了各领域需要通过数据出境安全评估的重要数据清单，涉及 18 个数据子类及其基本特征与描述。

二、 哪些行为属于数据跨境传输行为？

《评估申报指南（第二版）》和《标准合同备案指南（第二版）》第一部分“适用范围”明确了哪些行为属于“数据出境”，具体包含以下三种情形：

- 数据处理者将在境内运营中收集和产生的数据传输至境外；
- 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；
- 符合《个人信息保护法》第三条第二款情形（即在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，包括①以向境内自然人提供产品或者服务为目的、②分析、评估境内自然人的行为、③法律、行政法规规定的其他情形），以及在境外处理境内自然人其他数据处理活动。

（具体内容请见《下篇：实践篇》“二十二、如何准确识别数据跨境传输场景？”部分）

三、 如何定义出境数据的“境外接收方”？

根据《评估申报指南（第二版）》的规定，即使数据未转移存储至中国大陆以外的地方，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）的情形属于数据出境。同理，国内企业聘用境外服务供应商通过境外服务器直接收集于中国境内产生的个人信息，也属于数据出境。

“境外接收方”一般指第一手境外接收方，如果涉及多个境外第一手数据接收方，需在自评估报告中结合业务场景、数据出境规模、处理数据用途与方式以及数据接收方履行责任义务的管理和技术措施等因素，分别评估各接收方所具备的保障出境数据安全的能力。同时，如果数据出境后还会向其他境外接收方再传输数据，则也需要对该再传输行为进行评估。

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，并且多数为跨国公司总部直接委托境外供应商并签署数据处理协议（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）。在此背景下，如果境外母公司可以自行查阅、浏览存储于境外服务器的中国子公司的数据，并且数据处理协议约定境外母公司可以根据自己的目的对境外供应商收集的数据进行处理，则在此数据跨境传输过程中境外母公司属于境外接收方，中国子公司实质上是将个人信息跨境传输至其境外母公司。

四、 现行数据出境制度下的三条合规路径是什么？如何判断？

综合《网络安全法》《数据安全法》以及《个人信息保护法》这三大数据合规基本法律要求来看，企业开展数据出境活动时，应结合自身的主体类型、出境数据类型和数量，综合判断是否须要额外（1）申报并通过数据出境安全评估；或（2）订立并备案个人信息出境标准合同；或（3）通过个人信息保护认证。具体如下表所示：

<table>
<tr><th>法律名称</th><th>生效日期</th><th colspan="2">规制主体</th><th>合规路径</th></tr>
<tr><td>《网络安全法》</td><td>2017 年
6 月 1 日</td><td colspan="2">CIIO</td><td>向境外提供个人信息和重要数据，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。</td></tr>
<tr><td rowspan="2">《数据安全法》</td><td rowspan="2">2021 年
9 月 1 日</td><td colspan="2">CIIO</td><td>向境外提供重要数据，应当进行安全评估。</td></tr>
<tr><td colspan="2">CIIO 以外的数据处理者</td><td>向境外提供重要数据，遵照国家网信部门会同国务院有关部门制定的办法。</td></tr>
<tr><td rowspan="2">《个人信息保护法》</td><td rowspan="2">2021 年
11 月 1 日</td><td colspan="2">CIIO</td><td>向境外提供个人信息，应当进行安全评估。</td></tr>
<tr><td>CIIO 以外的数据处理者</td><td>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</td><td>向境外提供个人信息，应当进行安全评估。</td></tr>
</table>

			处理个人信息未达到国家网信部门规定数量的个人信息处理者	向境外提供个人信息，可以选择： （1）订立并备案个人信息出境标准合同；或 （2）通过个人信息安全保护认证。

表 1 我国数据合规三大法律规制下的数据出境制度

最新实施的《跨境流动规定》则对上述合规路径的适用范围进行了细化，提出：

1. 如果企业拟出境的数据符合《跨境流动规定》第三条、第四条、第五条和第六条规定的情形（以下合称**豁免情形**），则企业可依法依规自由开展数据出境活动。（具体内容请见《上篇：基础篇》“十二、哪些情况下不需要采取三大数据出境制度即可出境数据？”部分）若不符合豁免情形，则可继续参照下方第 2-4 项进行判断。

2. 如果企业是 CIIO，则应对其个人信息或重要数据的出境活动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。

3. 如果企业是 CIIO 以外的数据处理者，则首先应当结合相关部门、地区告知或者公开发布的情况判断拟出境的数据是否属于重要数据，出境数据属于重要数据的，则应当申报数据出境安全评估。

4. 如果企业是 CIIO 以外的数据处理者，出境的数据是个人信息，则：

   （1）自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息的，应当申报数据出境安全评估；

   （2）自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

为方便理解，企业可以参考如下图 1 总结的数据出境制度适用流程进行判断：

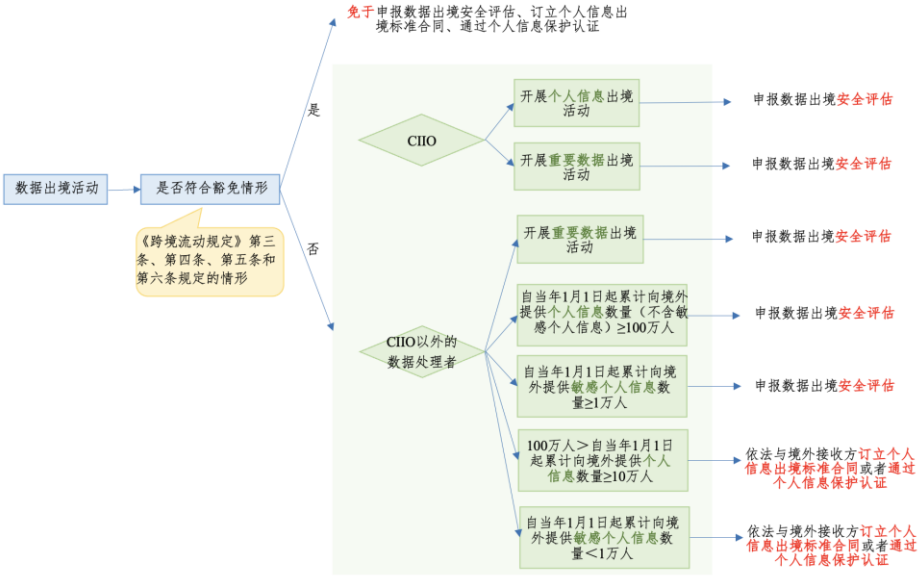


图 1 《跨境流动规定》下现行数据出境制度的适用流程

五、 哪些情况下需要申报数据出境安全评估？

最新发布的《跨境流动规定》适度收窄了数据出境安全评估范围。具体而言，根据《跨境流动规定》和《评估申报指南（第二版）》的规定，当数据处理者向境外提供数据不属于《跨境流动规定》下的豁免情形时（具体内容请见《上篇：基础篇》“十二、哪些情况下不需要采取三大数据出境制度即可出境数据？”部分），且具有下列情形之一时，应当申报数据出境安全评估：

1. CIIO 向境外提供个人信息或者重要数据；
2. CIIO 以外的数据处理者向境外提供重要数据；
3. CIIO 以外的数据处理者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）；
4. CIIO 以外的数据处理者自当年 1 月 1 日起累计向境外提供 1 万人以上敏感个人信息；

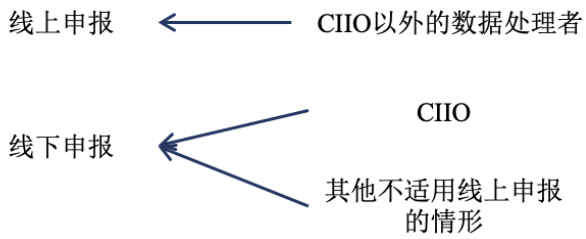
同时，《跨境流动规定》第六条规定，自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定本自贸区需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（下称**负面清单**），经

省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

六、 数据出境安全评估的流程是怎样的？

为指导数据处理者更好的开展数据出境安全评估申报工作，国家网信办结合此前申报工作开展的实践经验，发布了《评估申报指南（第二版）》并对数据处理者需要提交的相关材料进行了优化简化，同步开通了“数据出境申报系统”。

根据《评估申报指南（第二版）》，申报数据出境安全评估可分为线上申报和线下申报两种形式：（一）线上申报一般适用于 CIIO 以外的数据处理者申报数据出境安全评估，如该等数据处理者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）申报数据出境安全评估等场景；（二）CIIO 或者其他不适合通过线上系统申报数据出境安全评估的，应采取线下申报



流程。但是“不适合通过线上系统申报数据出境安全评估”的具体情形，仍待网信部门进一步澄清说明。

图 2 数据出境安全评估不同申报流程的适用范围

（一）线上申报流程

数据处理者进行数据出境安全评估的线上申报，应当通过线上数据出境申报系统提交申报材料，系统网址为 https://sjcj.cac.gov.cn。结合系统附带的《数据出境申报系统使用说明（第一版）》来看，数据出境申报系统整合统一了数据出境制度下的数据出境安全评估申报、个人信息出境标准合同备案工作，即该系统目前同时支持数据处理者申报数据出境安全评估、个人信息出境标准合同

备案；而对于个人信息保护认证，数据出境申报系统后续可能覆盖这一类数据出境制度的实施开展，但是相关功能仍在建设中，尚未上线。目前，申请个人信息保护认证可以登录个人信息保护认证管理系统，系统网址为 https://data.isccc.gov.cn[7]。

数据处理者在准备正式评估申报前，应根据《评估申报指南（第二版）》第三条和《数据出境申报系统使用说明（第一版）》准备以下文件：

- 统一社会信用代码证件影印件（加盖公章）
- 法定代表人身份证件影印件（加盖公章）
- 经办人身份证件影印件（加盖公章）
- 经办人授权委托书、承诺书
- 数据出境安全评估申报表
- 数据出境相关合同或者其他具有法律效力的文件影印件（加盖公章）
- 数据出境风险自评估报告扫描件

准备好以上材料后，数据处理者使用数据出境申报系统，应按照“注册用户账号→配置系统使用环境→选择新增评估填报入口”的流程进行数据出境安全评估申报：

1. 在注册用户账号阶段，数据处理者应准备好统一社会信用代码证、法人证件、系统注册人证件、注册授权书等材料扫描件或者照片。如果进行申报的实体为个人，可以勾选“无法人代表信息”跳过并进行后续填写。

2. 在配置系统使用环境阶段，数据处理者根据自身实际情况可以选择三种用户认证方式，即短信认证、使用专业浏览器加软证书结合认证、使用 Ukey 方式认证。

3. 点击“数据出境安全评估管理”-“新增评估”进入新增评估申报页面，上传安全评估材料，并在进入向导页面后，根据提示逐步完善申报信

[7] 参考网信中国，《促进和规范数据跨境流动规定》答记者问，https://mp.weixin.qq.com/s/-Y-dY_HL21jHTFQsMbeiVQ。

息，包括以下环节：

- 确认是否属于数据出境安全评估申报适用情形；
- 填写数据处理者情况；
- 填写法定代表人信息；
- 填写数据安全责任人和管理机构信息；
- 填写经办人信息；
- 填写数据处理者遵守中国法律、行政法规、部门规章情况；
- 填写数据出境场景；
- 上传其他数据出境安全评估申报材料。

（二）线下申报流程

CIIO 或者其他不适合通过线上系统申报数据出境安全评估的，应采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估，并按照《评估申报指南（第二版）》规定准备如下申报材料，将书面申报材料装订成册并附带材料电子版送达所在地省级网信办：

- 统一社会信用代码证件
- 法定代表人身份证件
- 经办人身份证件
- 经办人授权委托书
- 数据出境安全评估申报书
- 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
- 数据出境风险自评估报告
- 其他相关证明材料

七、 数据出境安全评估申报需要多长时间？

《评估申报指南（第二版）》未区分数据处理者进行数据出境安全评估线上申报和线下申报整体所需时间。一般情况下，数据出境安全评估的申报时长周期如图 3 所示：

图 3 数据出境安全评估申报时长周期

根据《评估申报指南（第二版）》第二条的规定，省级网信办会在收到申报材料之日起 5 个工作日内完成完备性查验，并向数据处理者告知查验结果。对于通过完备性查验的，省级网信办将申报材料提请国家网信办处理；对于未通过完备性查验的，省级网信办向数据处理者告知未通过完备性查验原因。

国家网信办自收到省级网信办提交的申报材料之日起 7 个工作日内，确定是否受理并书面通知数据处理者。根据《评估办法》第十二条的规定，国家网信办会在向数据处理者发出书面受理通知书之日起 45 个工作日内，完成数据出境安全评估。

在进行整体评估时，对于情况复杂或者需要补充、更正材料的情况，国家网信办会适当延长评估时间，并告知数据处理者预计延长的时间。数据处理者无正当理由不补充或者更正申报材料的，国家网信办可以终止安全评估。评估完成后，国家网信办向数据处理者出具评估结果通知书。数据处理者应当按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范相关数据出境活动。数据处理者对评估结果有异议的，可以在收到评估结果通知书 15 个工作日内向国家网信办申请复评，复评结果为最终结论。

八、 哪些情况下可以选择签署并备案个人信息出境标准合同？

《跨境流动规定》适当放宽了数据跨境流动条件，对以往应当订立个人信息出境标准合同的条件作了优化调整。具体而言，根据《跨境流动规定》和《标准合同备案指南（第二版）》的规定，企业同时符合下列情形，且不属于

《跨境流动规定》下的豁免情形时（具体内容请见《上篇：基础篇》“十二、哪些情况下不需要采取三大数据出境制度即可出境数据？”部分），可以通过签署并备案个人信息出境标准合同的方式向境外提供个人信息：

1. CIIO 以外的数据处理者；
2. 自当年 1 月 1 日起，累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）的；
3. 自当年 1 月 1 日起，累计向境外提供不满 1 万人敏感个人信息的。

需要说明的是，向境外提供被相关部门、地区告知或者公开发布为重要数据的个人信息，应当申报数据出境安全评估，不得选择订立个人信息出境标准合同或者通过个人信息保护认证的方式。

九、 个人信息出境标准合同的签署及备案流程是怎样的？

为指导和帮助个人信息处理者规范有序备案个人信息出境标准合同，国家网信办结合此前备案实践经验发布了《标准合同备案指南（第二版）》，并就个人信息出境标准合同备案的适用范围、备案方式、备案流程和材料以及咨询、举报联系方式等具体要求重新作出了优化说明。

标准合同备案流程可以总结为“开展个人信息保护影响评估并订立合同→材料提交→材料查验及反馈备案结果→补充或者重新备案→合同备案→开展个人信息出境活动”环节，时限和流程如下图 4 所示：

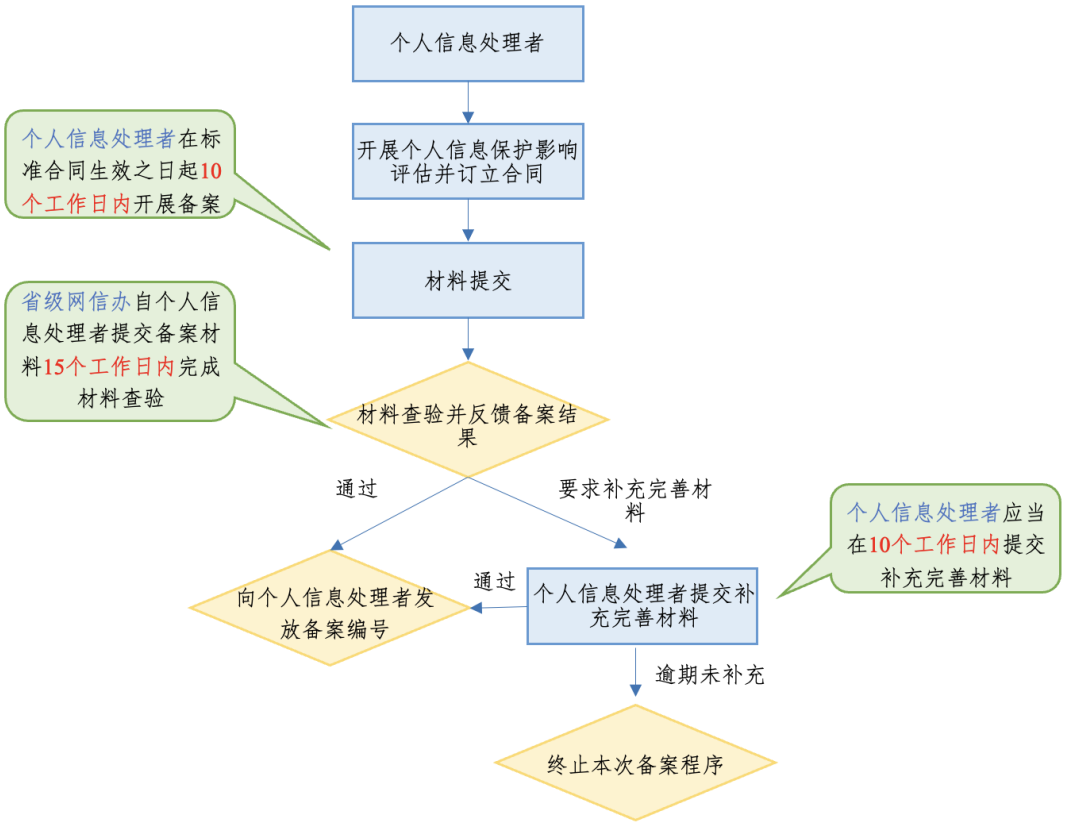


图 4 个人信息出境标准合同备案流程示意图

个人信息出境标准合同的签署及备案主要环节如下：

（一）开展个人信息保护影响评估并订立合同

首先，个人信息处理者在进行个人信息出境标准合同备案前，应开展个人信息保护影响评估。《个人信息保护法》第五十五条和《标准合同办法》第五条规定，向境外提供个人信息的，应当事前开展个人信息保护影响评估，并对处理情况进行记录。（具体内容请见《下篇：实践篇》“三十、如何开展个人信息保护影响评估？”部分）同时，企业应按照国家网信办发布的标准合同范本结合企业自身个人信息出境情况补充附录二，并与境外接收方订立标准合同。

（二）材料提交

由于以往的线下备案模式统一改为线上备案，故个人信息处理者应根据《标准合同办法》第七条和《标准合同备案指南（第二版）》在标准合同生效之日起 10 个工作日内，通过数据出境申报系统开展个人信息出境标准合同备案，系统网址为 https://sjcj.cac.gov.cn。根据《数据出境申报系统使用说明（第一

版)》，个人信息处理者使用数据出境申报系统，应按照“注册用户账号→配置系统使用环境→选择新增备案填报入口”的流程进行个人信息出境标准合同备案。

其中，注册用户账号和配置系统使用环境的具体操作流程和要求与数据出境安全评估申报相同（具体内容请见《上篇：基础篇》“六、数据出境安全评估的流程是怎样的？”部分）。

数据处理者登入系统后应选择“新增备案”进行个人信息出境标准合同备案。根据《标准合同备案指南（第二版）》和《数据出境申报系统使用说明（第一版）》，数据处理者备案个人信息出境标准合同备案，应提交以下文件：

- 统一社会信用代码证件影印件
- 法定代表人身份证件影印件
- 经办人身份证件影印件
- 经办人授权委托书
- 承诺书签字盖章的影印件
- 《个人信息出境标准合同》影印件（加盖公章）
- 《个人信息保护影响评估报告》影印件（加盖公章）

在实际使用数据出境申报系统进行备案的过程中，企业应通过页面向导，逐步完善备案信息，包括以下环节：

- 确认个人信息出境标准合同适用情形
- 填写个人信息处理者基本情况；
- 填写法定代表人信息；
- 填写经办人信息；
- 上传承诺书签字盖章的影印件；
- 填写个人信息处理者遵守中国法律、行政法规、部门规章情况；
- 填写个人信息出境场景；
- 上传《个人信息出境标准合同》加盖公章的影印件，并填写相关信息；
- 上传《个人信息保护影响评估报告》加盖公章的影印件；
- 上传其他相关证明材料。

（三）材料查验及反馈备案结果

个人信息处理者完成材料提交后，整体备案流程进入了材料查验及反馈备案结果阶段。根据《标准合同备案指南（第二版）》第三条的规定，省级网信办应当自个人信息处理者提交备案材料之日起 15 个工作日内完成材料查验，并向符合备案要求的个人信息处理者发放备案编号。需要补充完善材料的，个人信息处理者应当在 10 个工作日内提交补充完善材料；逾期未补充完善材料的，可以终止本次备案程序。

十、 哪些情况下可以选择个人信息保护认证？

与签署并备案个人信息出境标准合同的情况一样，可以选择个人信息保护认证的情形亦发生了变化。具体而言，根据《跨境流动规定》的规定，企业在符合以下条件之一，且不属于《跨境流动规定》下的豁免情形时（具体内容请见《上篇：基础篇》“十二、哪些情况下不需要采取三大数据出境制度即可出境数据？”部分），可以通过开展个人信息保护认证的方式向境外提供个人信息：

1. CIIO 以外的数据处理者自当年 1 月 1 日起，累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）的；

2. CIIO 以外的数据处理者自当年 1 月 1 日起，累计向境外提供不满 1 万人敏感个人信息的。

需要说明的是，向境外提供被相关部门、地区告知或者公开发布为重要数据的个人信息，应当申报数据出境安全评估，不得选择订立个人信息出境标准合同或者通过个人信息保护认证的方式。

十一、 进行个人信息保护认证的流程是怎样的？

2022 年 11 月 18 日，国家市场监督管理总局和国家网信办发布的《认证公告》以及附件《认证规则》，对开展个人信息保护认证的流程进行了细节说明，

包括认证委托、技术验证、现场审核、认证结果评价和批准等环节。《认证公告》指出“从事个人信息保护认证工作的认证机构应当经批准后开展有关认证活动”。虽然，相关法律法规并未明确公布依法取得认证机构资质的企业名录，但根据向中国网络安全审查认证和市场监管大数据中心（下称**网安审认证和市监大数据中心**）咨询的结果以及国家网信办于 2024 年 3 月 22 日发布的《<促进和规范数据跨境流动规定>答记者问》，企业可以通过个人信息保护认证管理系统（具体网址为 https://data.isccc.gov.cn）向网安审认证和市监大数据中心进行申请（具体内容请见《下篇：实践篇》“四十、企业应当向哪个/些机构申请个人信息保护认证？”部分）。

同时，《跨境认证要求（征）》具体规定了在个人信息跨境传输场景下开展个人信息保护认证的适用情形、基本原则以及基本要求，为认证机构对个人信息跨境处理活动开展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合规开展个人信息跨境处理活动提供了参考。

开展个人信息保护认证包括“认证委托、技术验证、现场审核、认证结果评价和批准、获证后监督”五个环节，具体流程如图 5 所示：

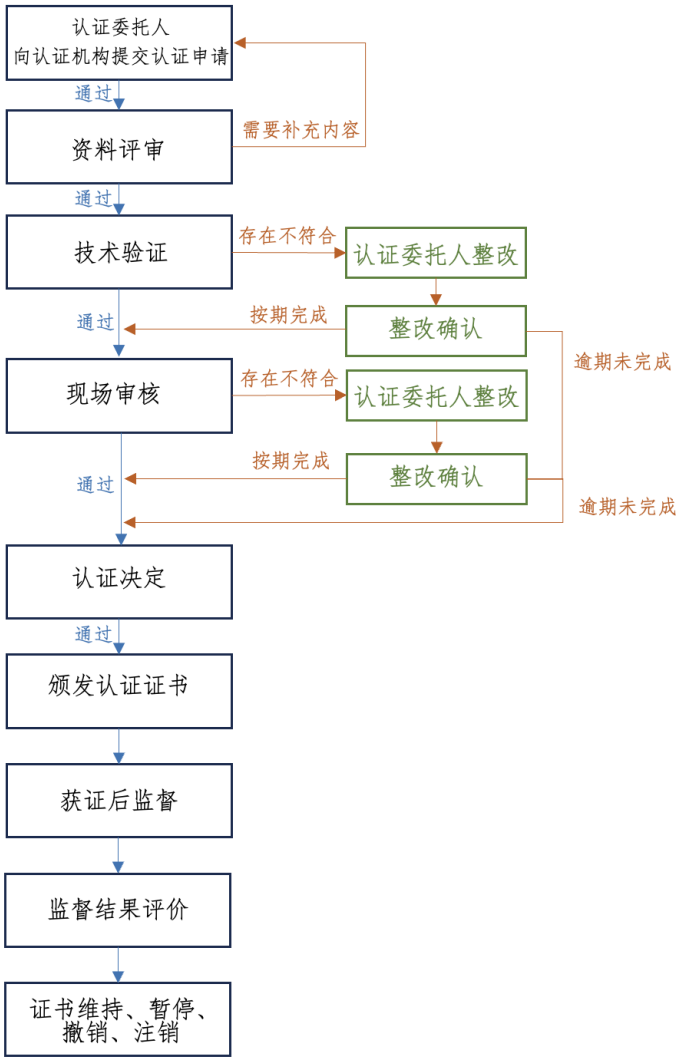


图 5 个人信息保护认证流程示意图

首先，个人信息处理者（即认证委托人）应当按认证机构的要求提交认证委托资料，包括但不限于认证委托人基本材料、认证委托书、相关证明文档等。认证委托人在申请个人信息保护认证前可以按照认证依据的要求开展自评估以及合规整改，以符合认证依据的有关要求。

认证机构在对认证委托资料审查后及时反馈是否受理。认证机构会根据认证委托资料确定认证方案，包括个人信息类型和数量、涉及的个人信息处理活

动范围、技术验证机构信息等，并通知认证委托人[8]。

通过后，技术验证机构会按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告[9]。认证机构会进行现场审核，并向认证委托人出具现场审核报告[10]。

认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，认证机构会颁发认证证书；对暂不符合认证要求的，认证机构有权要求认证委托人限期整改；对于整改后仍不符合的，认证机构有权以书面形式通知认证委托人终止认证。认证机构如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

认证机构在认证有效期内，会对获得认证的个人信息处理者进行持续监督，确保获得认证的个人信息处理者持续符合认证要求。认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

十二、 哪些情况下不需要采取三大数据出境制度即可出境数据？

《跨境流动规定》第三、四、五、六条明确提出了免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的豁免情形，具体包括：

（一）个人信息过境

根据《跨境流动规定》第四条，在境外收集和产生的个人信息传输至境内处理后向境外提供，若处理过程中没有引入境内个人信息或者重要数据的，则不再需要采取额外的数据出境制度。例如，某国内电商平台在境外设有物流仓库，并与境外的物流公司和航空公司合作。境外消费者在该平台国际站购买商

[8] 《认证规则》第 4.1 条。
[9] 《认证规则》第 4.2 条。
[10] 《认证规则》第 4.3 条。

品后，平台内商家负责将商品整理发货，由境外物流公司和国外航空公司承运，运输商品并交付消费者。在这个流程中，境内电商平台、平台内商家、物流公司和航空公司等参与方均会涉及处理消费者个人信息。在此过程中，境外消费者的订单信息是由国内电商平台的境外站收集后入境的，用户账号也由该平台国际站负责运营管理，境外消费者的个人信息收集活动不发生在境内，且入境后的处理过程未引入境内消费者的个人信息，经过平台确认交易订单信息后发送给境外的物流公司和航空公司进行运输配送。所以，根据《跨境流动规定》第四条的规定，针对上述境外个人信息入境再出境的情形，电商平台无需采取额外的数据出境制度，提高了跨境电商的服务效率。

（二）基于人力资源管理出境员工个人信息所确需

根据《跨境流动规定》第五条第一款第二项规定，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，确需向境外提供内部员工个人信息的，不需要采取额外的数据出境制度。但是，若企业希望依据该场景豁免采取数据出境制度，则需要重点排查并关注自身数据出境活动，确保跨境传输员工个人信息的行为是为实施人力资源管理所“确需”的、特定字段的出境也是为实施人力资源管理所“确需”的。

（三）为订立、履行个人作为一方当事人的合同所确需

根据《跨境流动规定》第五条第一款第一项规定，符合“为订立、履行个人作为一方当事人的合同所必需”这一前提，确需向境外提供个人信息的，不需要采取额外的数据出境制度。本条针对“履行合同所必需”进行了场景上的罗列，例如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等需要向境外提供个人信息的情形。例如，消费者投资国际金融产品时，为了满足合同的要求、法律规定或者行业监管要求，要向境外提供个人信息，如投资人姓名、身份证信息、联系方式、财务状况等。

（四）紧急情况下为保护自然人的生命健康和财产安全所确需

根据《跨境流动规定》第五条第一款第三项规定，“紧急情况下为保护自然人的生命健康和财产安全等”确需向境外提供个人信息的，不需要采取额外的

数据出境制度。例如，某国家发生了突发性疫情，为了挽救已受影响的人民群众的生命安全，某些组织可能需要将患者的个人信息发送给国际救援机构，以便及时确定该突发疫情形成的原因、在其他国家或地区是否已有发生和确认其相似度、受灾地区的药品供应情况并采取必要的救援措施等。此条旨在保障救援资源的合理配置和人民群众的生命安全。

（五）国际贸易

根据《跨境流动规定》第三条规定，国际贸易活动中收集和产生的数据出境，不包含个人信息或者重要数据的，不需要采取额外的数据出境制度。例如，当某国内外贸企业向他国出口商品时，需要将商品的数量、规格、重量、价值以及运输方式等信息发送至进口方，以便各国的海关、物流公司和贸易伙伴对这批出口货物的运输和交付进行管理。但是“国际贸易”概念的外延十分宽泛。其中，何种类型的商业活动属于“国际贸易”的范畴、哪些实践中的流程环节属于“国际贸易”以及境外数据接收方是否仅限于贸易相对方等问题还待进一步解释说明。

（六）跨境运输

根据《跨境流动规定》第三条规定，跨境运输活动中收集和产生的数据出境，不包含个人信息或重要数据的，不需要采取额外的数据出境制度。例如，比较常见的是，境内消费者在电商平台购买了境外商家的商品，商家发货地位于境外，需要将商品从境外跨境运输至国内，这一过程可能涉及平台方将境内消费者的收件地址、联系方式等个人信息提供给境外的国际承运人来完成商品的跨境运输。但类似于场景（五），“跨境运输”的概念较为广泛，不仅涉及日常电商平台交易相关的货品运输，还可能涉及到更为复杂的运输场景，如矿石资源、农产品、原油等非零售的大宗商品国际长途运输，这些场景是否均可以被纳入到豁免范围内，仍有待在实践中进一步探索。

（七）学术合作

根据《跨境流动规定》第三条规定，学术合作活动中收集和产生的不包含个人信息或重要数据的一般数据出境活动，不需要采取额外的数据出境制度。

例如，国内某高校研究所与其他国家或机构的研究人员合作进行学术研究，可能需要共享一些数据，例如实验结果、调查结论、统计数据等，不包含个人信息或重要数据。学术相关数据的跨境传输可以推动国际学术界的合作与交流，促进全球科学研究发展。但是，与场景（五）相似，学术合作场景行业领域的适用性较为宽泛，某些行业领域的数据，即使不属于个人信息或是重要数据，但是大规模的统计数据或是敏感数据，可能会构成“情报”、“国家秘密”等。同时，如何在学术合作场景中鉴别被共享的学术数据不涉及重要数据或者国家秘密，也是一项技术性很强的工作。因此，此类场景适用豁免规定需要特别小心，以防发生可能会危害到国家安全与社会利益的情况。

（八）跨国生产制造

根据《跨境流动规定》第三条规定，跨国生产制造活动中收集和产生的不包含个人信息或重要数据的一般数据出境活动，同样也不需要采取额外的数据出境制度。例如一家制造业的国企在全球多个国家设有生产基地，在进行产品生产制造和装配时，为对全球生产基地进行有效供应链管理、确保物料的及时供应，涉及物料库存管理信息、零部件生产计划、物流运输信息等数据需要提供给海外基地。但类似于场景（五），“跨国生产制造”的概念较为广泛，涉及的环节也较多、程序繁琐、参与方多样，数据出境的链条也可能相对复杂。因此，企业仍需在实践中进一步探索合规落地标准，同时也建议企业及时就“可疑问题”与监管机构多沟通。

（九）跨国市场营销

根据《跨境流动规定》第三条规定，跨国营销活动中收集和产生的不包含个人信息或重要数据的一般数据出境活动，不需要采取额外的数据出境制度。例如，跨国消费品企业拟进入我国市场或扩大其在中国市场的业务前都会对国内市场进行调研。为此，企业必然需要收集和分析一些市场数据，包括我国各线市场调研报告、同行市场占比分析数据、消费者行为数据等，以充分了解目标市场的消费者需求、竞争情况、市场趋势等。通过收集相关境内市场数据，该跨国公司可以更好地了解和把握我国目标市场的特点和机会，制定相应的市场营销策略和计划，有助于支持公司在我国的市场营销决策和推广活动，进一

步促进我国经济发展。

（十）其他一般数据

除了场景（五）至场景（九）列举的各种情况，《跨境流动规定》第三条对不包含个人信息或者重要数据的一般数据进行了兜底性质的描述—即在国际贸易、跨境运输、学术合作、跨国生产制造和市场营销“等活动”中出境一般数据，不需要采取额外的数据出境制度。然而，是否所有类似活动下的一般数据均能自由跨境流动？如何确定“等活动”的具体范围？实践中其他活动如何能类推适用第三条的豁免规定？这些细节问题仍待结合监管实践案例进一步补充说明。

（十一）“自贸区负面清单”数据

《跨境流动规定》除了明确提及以上十大场景外，还专门设计了“自贸区负面清单”的特殊机制，即自由贸易试验区在国家数据分类分级保护制度框架下，可自行制定本自贸区需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单，报经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。自贸区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

十三、 哪些情形属于“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》以及《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》第三十七条规定，机关、单位向境外或者向境外在中国境内设立的组织、机构提供国家秘密，任用、聘用的境外人员因工作需要知悉国家秘密的，按照国家有关规定办理。根据第四十二条规定，采购涉及国家秘密的货物、服务的机关、单位，直接涉及国家秘密的工程建设、

设计、施工、监理等单位，应当遵守国家保密规定。机关、单位委托企业事业单位从事涉及国家秘密的业务，应当与其签订保密协议，提出保密要求，采取保密措施。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）》第三十条规定，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》第三十四条规定，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》第五十七条规定，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。

十四、 CIIO数据出境的要求有哪些？

CIIO 包括电信运营商、金融机构、能源供应商等，其掌握大量的个人信息和重要数据。这些数据的安全性对于国家和个人都至关重要。例如，金融机构处理客户的财务信息，电信运营商处理用户的通信数据，能源供应商掌握能源供应和分配的关键数据。通过对 CIIO 向境外提供的个人信息和重要数据进行监管，可以防止这些数据被滥用、泄露或用于不法目的。

我国现行有效的法律对于 CIIO 的数据出境活动进行了明确规制。《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。可以看出，由于 CIIO 数据的泄露、破坏、丢失等将可能对国家安全、社会公共利益和个人隐私产生重大影响，我国对 CIIO 的数据出境活动采取了严格把控的态度。

但需要注意的是，《跨境流动规定》第七条在明确 CIIO 申报数据出境安全评估的条件的同时，规定了“属于第三条、第四条、第五条、第六条规定情形

的，从其规定”。《跨境流动规定》第五条第一款第（一）至（三）项列出了数据处理者向境外提供个人信息免于采取数据出境制度的三种情形，即（i）为订立、履行个人作为一方当事人的合同，向境外提供个人信息；（ii）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跨境人力资源管理，向境外提供员工个人信息；及（iii）紧急情况下为保护自然人的生命健康和财产安全，向境外提供个人信息的。因此，若 CIIO 向境外提供个人信息属于上述三种情况的，可以依照上述规定免于申报数据出境安全评估。

虽然目前大多数企业并未被认定为 CIIO，以上规定对它们的直接影响相对较小，但这些企业也需要关注其客户或合作方是否有可能属于 CIIO。企业在与 CIIO 进行业务活动时，需要特别遵守 CIIO 进行跨境数据交互的合规义务。

十五、 识别重要数据的法律法规依据有哪些？

为确保数据安全和维护国家利益，重要数据跨境传输已成为各国或各地区关注的规制焦点。我国监管部门也明确要求企业不仅需要对于“重要数据”的出境活动开展风险自评估工作，还需要向网信部门申报数据出境安全评估，以加强对数据跨境传输的监管，确保数据的安全。

《数据安全法》第二十一条规定，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。顺应这一要求，GB/T 43697-2024《数据安全技术 数据分类分级规则》在 2024 年 3 月 15 日正式发布，其中第 6.5 b）条及附录 G《重要数据识别指南》在国家总体宏观层面给出了明确的重要数据判断标准，即满足以下任一条件的数据，识别为重要数据：（i）数据一旦遭到泄露、篡改、损坏或者非法获取、非法使用、非法共享，直接对**国家安全**造成**一般危害**；（ii）数据一旦遭到泄露、篡改、损坏或者非法获取、非法使用、非法共享，直接对**经济运行**造成**严重危害**；（iii）数据一旦遭到泄露、篡改、损坏或者非法获取、非法使用、非法共享，直接对**社会秩序**造成**严重危害**（如影响社会稳定）；（iv）数据一旦遭到泄露、篡改、损坏或者非法获取、非法使用、非法共享，直接对**公共利益**造成**严重危害**（如危害公共健康和安全）；

（v）数据**直接关系**国家安全、经济运行、社会稳定、公共健康和安全的**特定领域、特定群体或特定区域**；（vi）数据达到一定精度、规模、深度或重要性，**直接影响国家安全、经济运行、社会稳定、公共健康和安全**；以及（vii）经行业领域主管（监管）部门评估确定的重要数据。此外，各地区、各部门也在抓紧推进确立本地区、本部门以及相关行业、领域的重要数据具体目录，为企业提供更具普适性和可操作性的重要数据识别规范，以重点保护列入目录的数据。

因此，尽管法律法规对“重要数据”进行了定义，也从国家宏观角度提供了识别指南规范，但各地区、各行业的重要数据目录仍未出台，企业在实际操作过程中，如何界定重要数据仍然存在一定的模糊性。对此，《跨境流动规定》第二条提出了明确指引，采用与判断企业是否属于 CIIO 同一方法，即以地方和行业主管部门的告知为标准。企业仅需注意相关部门、地区是否已经告知或者是否已经公开发布了本企业所处理的数据属于重要数据，这一定程度上减轻了企业的合规压力，缓解了识别重要数据“难”的问题。因此，建议企业后续不断关注各主管部门可能陆续发布的“重要数据”目录和清单，并对本企业拟出境数据合规性进行阶段性确认，与各主管部门能够保持积极且透明地沟通，及时调整数据跨境策略，以避免潜在的合规风险。

十六、 重要数据出境的要求有哪些？

数据处理者向境外提供重要数据，需申报数据出境安全评估[11]。（具体内容请见《上篇：基础篇》“六、数据出境安全评估的流程是怎样的？”部分）

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等[12]。（具体内容请见《下篇：实践篇》“三十一、如何开展数据出境风险自评估？”部分）

[11] 《评估办法》第四条。
[12] 《评估办法》第五条。

十七、 个人信息出境标准合同的具体内容有哪些？

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。

根据《标准合同办法》附件，目前版本的标准合同内容主要包括：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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；
6. 救济、合同解除、违约责任、争议解决等。

由于个人信息出境属于个人信息处理活动中的一种情形，因此个人信息出境应当遵循《个人信息保护法》规定的个人信息处理活动的基本要求，标准合同的部分条款也体现了《个人信息保护法》下个人信息处理活动的一般原则。此外，标准合同规定了出境方与接收方跨境传输个人信息时应当履行的义务，但是未针对双方在数据处理活动中的权利义务如何分配作出具体要求，这些内容可由双方通过附件或者其他合同进行补充细化。需要注意的是，根据《标准合同办法》第六条的规定，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。对于合同双方在签订标准合同之前就数据跨境传输已签署了相关协议的情况，若相关协议条款与标准合同相冲突，标准合同的条款应优先适用。

十八、 进行个人信息保护认证的具体要求有哪些？

个人信息保护认证定位为国推自愿性认证，鼓励符合条件的个人信息处理者对开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等处理活动自愿申请个人信息保护认证。就“自愿认证”而言，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。如果选择认证，也需要判断是否符合需申报数据出境安全评估的情形。若符合，个人信息处理者则必须进行数据出境安全评估申报。

根据《认证规则》，个人信息保护认证依据为 GB/T 35273-2020《信息安全技术 个人信息安全规范》，对于开展跨境处理活动的个人信息处理者，还应当符合《认证规范 V2.0》的要求。上述标准、规范原则上应当执行最新版本。

注册于（适用于组织)/位于(适用于个人)粤港澳大湾区内的个人信息处理者，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市及香港特别行政区的个人信息处理者跨境处理个人信息则应当符合《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿)》的相关要求。该指南共包含六部分内容，即范围、术语定义、个人信息处理要求、基本原则、个人信息权益保障要求以及个人信息安全要求。指南在强调重述《个人信息保护法》各项要求的同时，还融入了香港《个人资料（私隐）条例》的相关规定，例如使用个人信息进行商业营销需征得个人信息主体的同意等。

GB/T 35273-2020《信息安全技术 个人信息安全规范》从个人信息收集、个人信息存储、个人信息使用、个人信息主体的权利、个人信息的委托处理、共享、转让、公开披露、个人信息安全事件处置以及组织的个人信息安全管理要求等七个方面规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。

此外，对于开展个人信息跨境处理活动，《跨境认证要求（征)》从具有法律约束力的文件、组织管理、个人信息跨境处理规则、个人信息保护影响评估、个人信息主体权利、个人信息处理者以及境外接收方的责任义务等六

个方面对个人信息处理者提出了基本要求，包括：

1. 个人信息处理者与境外接收方签署具有法律约束力和可执行的文件，确保个人信息主体权益得到充分保障；
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指定个人信息保护负责人，并设立个人信息保护机构；
3. 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约定并共同遵守同一个人信息跨境处理规则；
4. 个人信息处理者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，并形成个人信息保护影响评估报告；
5. 个人信息处理者和境外接收方应响应个人信息主体的有关权益；
6. 个人信息处理者和境外接收方应履行相应的责任义务。

这些要求不仅可以作为认证机构实施个人信息跨境处理活动认证的相关依据，也可以为个人信息处理者规范其个人信息跨境处理活动提供参考。

十九、 未符合数据出境制度，有何罚则？

《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，具体而言：

根据《网络安全法》第六十六条，CIIO 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，未履行相关合规流程的，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。同时，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。

根据《中华人民共和国刑法》（下称**《刑法》**）第二百五十三条之一，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

二十、 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》，违反法律规定跨境传输国家秘密的，有可能构成犯罪并需承担刑事责任。

除此之外，企业还应当关注《刑法》规定的刑事责任，如《刑法》第一百一十一条规定，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、管制或者剥夺政治权利。

若涉及某特定领域或行业，公司还需要检索相关行业的法律法规、部门规章及其他规范性文件以确认是否存在适用的特殊规定，以避免受到处罚。

二十一、 我国粤港澳大湾区就个人信息出境是否有特殊便利措施？

2023 年 6 月 29 日，香港创新科技及工业局与国家网信办签署《促进粤港澳大湾区数据跨境流动的合作备忘录》（下称《合作备忘录》），以降低跨境数据流动的合规成本，促进大湾区数字经济及科研发展。

为落实《合作备忘录》，香港创新科技及工业局与国家网信办于 2023 年 12 月 13 日共同发布《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》（下称**《实施指引》**），《实施指引》明确，粤港澳大湾区个人信息处理者及接收方可以按照《实施指引》要求，通过订立《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》（下称**《大湾区标准合同》**）的方式进行粤港澳大湾区中内地和香港之间的个人信息跨境流动（被相关部门、地区告知或者公开发布为重要数据的个人信息除外）。

《大湾区标准合同》适用于个人信息处理者及接收方注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地九个城市（即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市及肇庆市）和香港之间的个人信息跨境流动，即既包括由大湾区内地城市至香港的个人信息跨境流动，也包括由香港至大湾区内地城市的个人资料跨境流动，但并不适用内地与澳门之间的个人信息跨境流动。

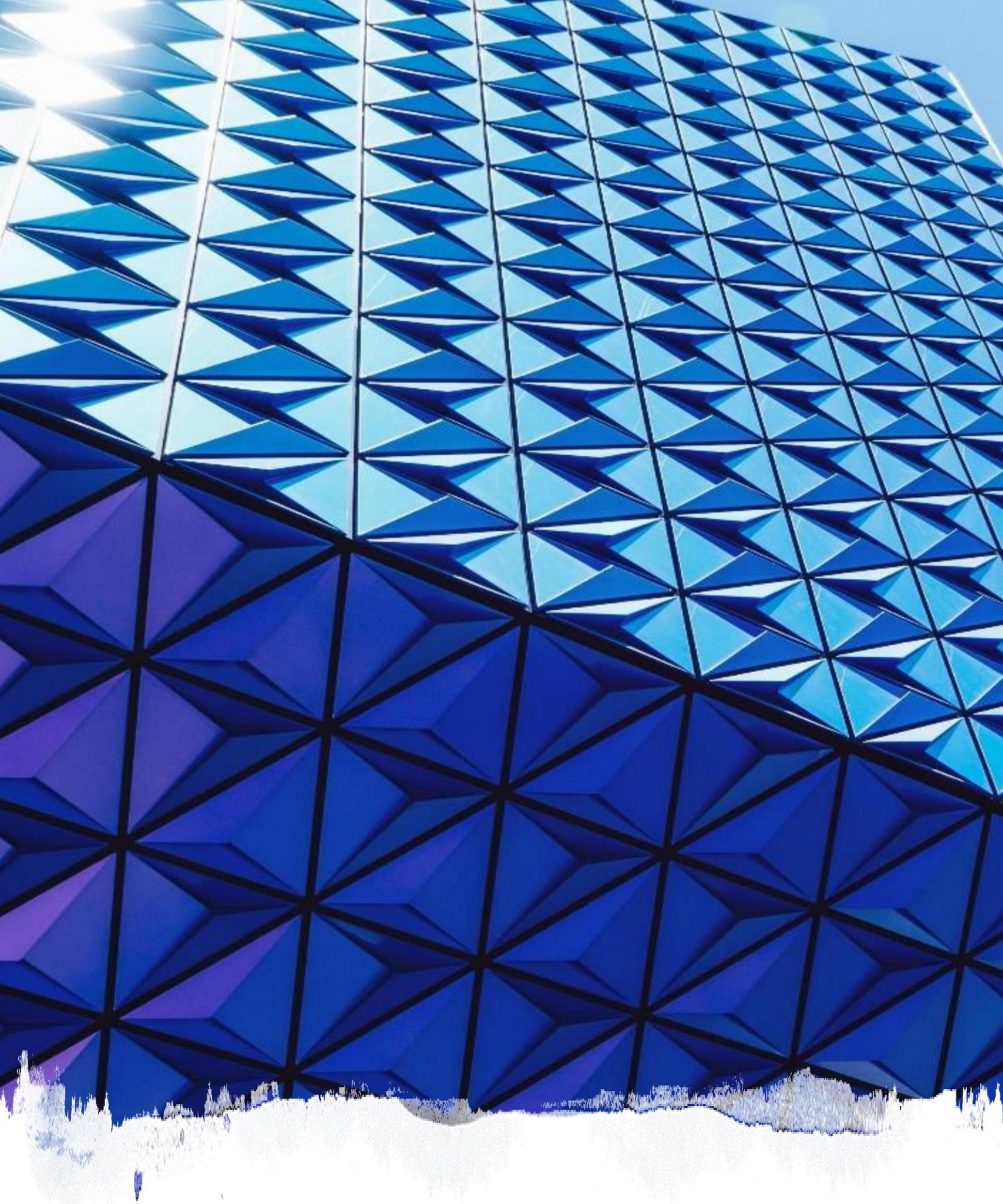
根据香港特区政府资讯科技总监办公室的说明，《大湾区标准合同》是一项简化大湾区中内地地区与香港之间的个人信息跨境流动活动合规安排的措施，属自愿性质，让两地的个人及机构按统一范本订立标准合同，规范合同双方在个人信息保护方面的责任和义务。通过《大湾区标准合同》约定跨境流动的个人信息，不得再向粤港澳大湾区以外的组织或者个人提供。

值得注意的是，签署《大湾区标准合同》的个人信息处理者及接收方应在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者香

港特区政府资讯科技总监办公室进行标准合同备案，并提交法定代表人身份证件影印件、承诺书、标准合同。

与内地标准合同的备案要求相比，《大湾区标准合同》备案虽然免除了提交个人信息保护影响评估报告的义务，但仍要求企业自主开展个人信息保护影响评估工作并基于评估结果作出合规承诺，因此对于签订《大湾区标准合同》的个人信息处理者来说，开展个人信息保护影响评估更多的是作为加强企业自身风险管理能力的有效工具。《大湾区标准合同》对于备案程序的简化一方面为大湾区组织及个人的个人信息跨境流动活动提供了便利，另一方面也没有完全放松对相关组织及个人开展个人信息保护影响评估工作的要求。

由此，开展数据跨境流动活动的大湾区企业可以在满足《实施指引》规定的前提下考虑与区域内的相关方签署《大湾区标准合同》以增强出境活动的合规性和便利性，但同时企业也应当注意履行相关的个人信息保护合规义务以避免触碰监管红线。



下篇：实践篇

二十二、 如何准确识别数据跨境传输场景？

结合《评估申报指南（第二版）》和《标准合同备案指南（第二版）》明确了哪些行为属于“数据出境”，包含（一）数据处理者将在境内运营中收集和产生的数据传输至境外；（二）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；（三）在中华人民共和国境外处理境内自然人个人信息等其他数据处理活动。（具体内容请见《上篇：基础篇》“二、哪些行为属于数据跨境传输行为？”部分）

因此，在判断是否涉及“数据出境”时，企业需要重点关注：

1. 该等数据是否在“境内运营过程中”收集和产生；
2. 企业的行为是否属于“向境外提供”，或可以被境外“查询、调取、下载、导出”；以及
3. 在境外处理境内自然人个人信息等其他数据处理活动，是否符合《个人信息保护法》第三条第二款情形，即在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，包括①以向境内自然人提供产品或者服务为目的、②分析、评估境内自然人的行为、③法律、行政法规规定的其他情形。

（一）是否在“境内运营过程中”收集和产生

在判断数据是否属于在“境内运营过程中”收集和产生前，应厘清“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。“国境内”指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（以下合称**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[13]。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。

13 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。

在这种定义下港澳台地区属于“境外”范围。《网安条例（征）》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。从该条规定可以推断出，数据跨境相关法律法规在对“境内”的进行定义时也倾向从“关境内”的角度进行解释，即认为由中国大陆向港澳台地区传输数据的行为属于“出境”行为。

对于“境内运营”，目前行业内普遍认为，“境内运营”是指网络运营者在中国境内开展业务，提供产品或服务。实践中，若企业运营的产品仅向境外提供服务，且不收集境内数据，此种情况不属于“境内运营”。同时，如果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，不涉及处理境内的个人信息和重要数据，此种场景也不纳入“境内运营”的范围。

（二）是否属于三种典型数据出境行为

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：

a) 通过具有数据传递功能的介质向境外提供数据（图 6）

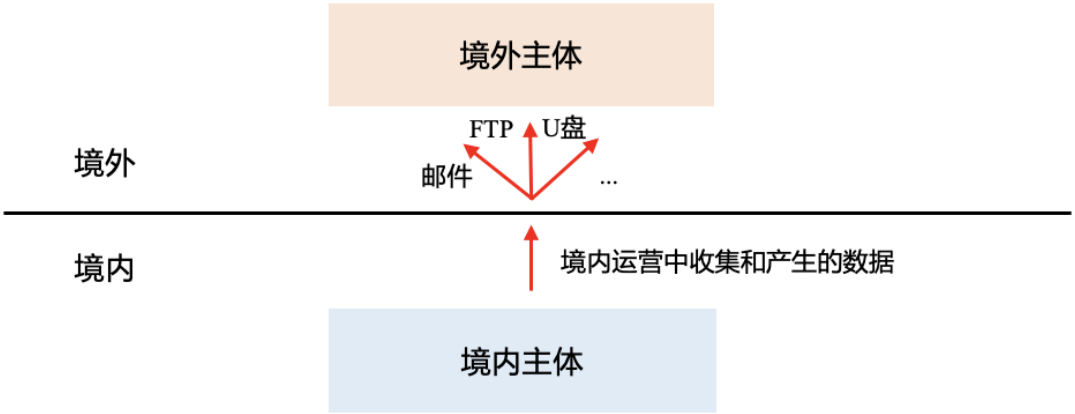


图 6

具有数据传递功能的软件或硬件等物理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。该场景属于较容易识别的数据出境场景。

b) 将数据上传或存储至位于境外的服务器或云端（图 7）

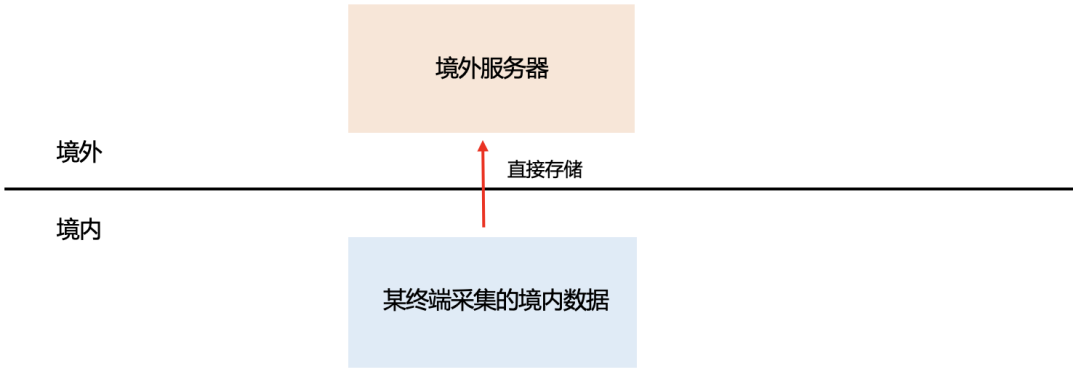


图 7

如果企业使用的信息系统、软件平台或数据库的服务器或云端部署在境外（如跨国企业使用境外服务商运营及/或部署的信息系统），也会构成境内主体主动向境外传输数据。

c) 经由第三方向境外传输数据（图 8）

此外，境内主体和境外主体之间的数据传输活动往往还会涉及第三方。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。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，并因此很可能被认定是数据的境外接收方。

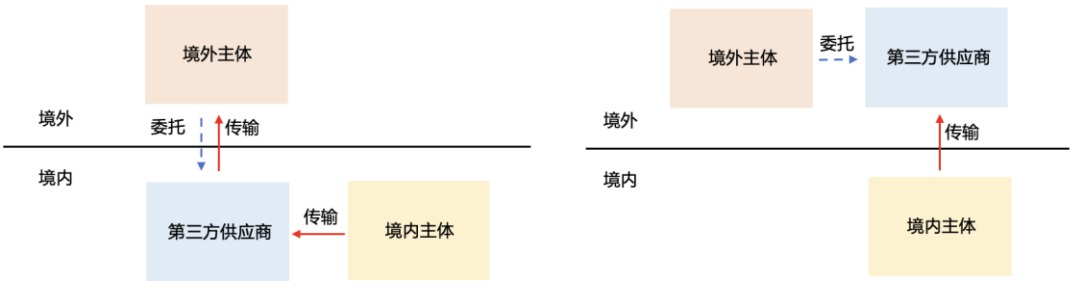


图 8

2. 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（公开信息、网页访问除外）

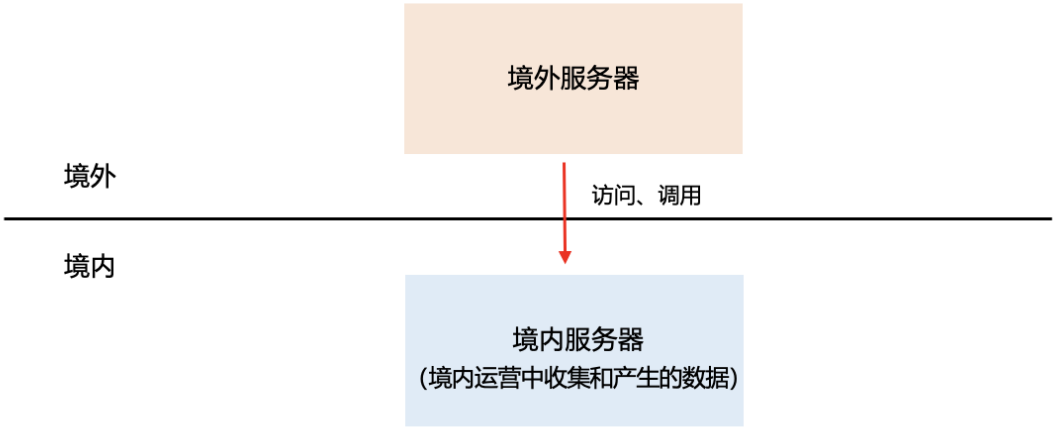


图 9

在判断是否属于数据出境行为时，也应关注“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，只要存在境外数据处理者查询、调取、下载、导出于境内运营中产生的数据的情况，则属于数据出境（如图 9）。

由此可见，跨国公司、同一经济/事业实体下属子公司或者关联公司访问、调用、下载、导出存储于境内数据的行为也属于数据出境。例如，外国公司在中国投资设立的企业（即 **FIE**）的境外母公司对 FIE 存储于中国服务器中相关数据进行访问的行为属于数据出境。

3. 在境外处理境内自然人个人信息等其他数据处理活动

除“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”和“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”外，《评估申报指南（第二版）》和《标准合同备案指南（第二版）》明确提出了第三种出境行为：“符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他个人信息处理活动”。

具体而言，《个人信息保护法》第三条第二款规定，“在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。”

对于“以向境内自然人提供产品或者服务为目的”，可以理解为以我国为目标市场并以个人为对象的跨境交易。对于相关境外个人信息处理者是否以我国为目标市场，应当综合多种因素对其商业意图进行判断，如境外处理者的网站、应用程序使用中文对相关产品和服务进行标识、介绍；将人民币作为支付货币或者接入我国境内支付工具等，可以表明该境外处理者将我国作为目标市场[14]。

对于“分析、评估境内自然人的行为”，与《通用数据保护条例》（欧盟第 2016/679 号条例）（下称 **GDPR**）下“监控”（Monitoring of EU Customers' Behaviour）的概念类似[15]。GDPR Recital 24 中规定“为了确定处理活动是否可以被视为监控，需要确定自然人是否在互联网上被跟踪记录，或者潜在地后续使用个人数据处理技术，包括对自然人进行数据画像特别是做出自动化决策，或者对其个人偏好、行为或态度做出分析或预测”。参考上述概念，“分析、评估”可以理解为通过持续记录、追踪相关个人信息，并通过后续的处理技术，对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等作出分析或预测[16]。例如，一名中国用户浏览某招聘平台的国际版网站查看海外求职市场的招聘信息，并注册了用户账号。位于美国的该平台总部对该名中国用户的个人信息进行了分析、评估，并在此基础上向其发送了求职工作岗位相关的个性化推送。此种场景符合在中国境外“分析、评估境内自然人的行为”，因此属于数据出境行为。

而“法律、行政法规规定的其他情形”为兜底性条款。考虑到新技术新应用的发展可能为规制个人信息处理活动带来挑战，兜底性条款为相关法律、行政法规应对跨境处理活动管理过程中出现的新问题，提供了必要的适用空间与灵活性。

二十三、 企业可能涉及的数据跨境传输场景有哪些？

（一）人力资源数据出境场景

[14] 参考全国人大常委会法工委经济法室的立法专家杨合庆主编的《个人信息保护法释义》，北京：法律出版社，2022。
[15] 参考程啸主编的《个人信息保护法理解与适用》，北京：中国法制出版社，2021。
[16] 参考法律出版社法规中心《中华人民共和国个人信息保护法注释本》，北京：法律出版社，2022。

1. 公司招聘（应聘者个人信息出境）

以外企为例，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：

a) **境外总部企业官网统一招聘员工，由应聘人员直接访问境外网站填写个人信息（图 10）**

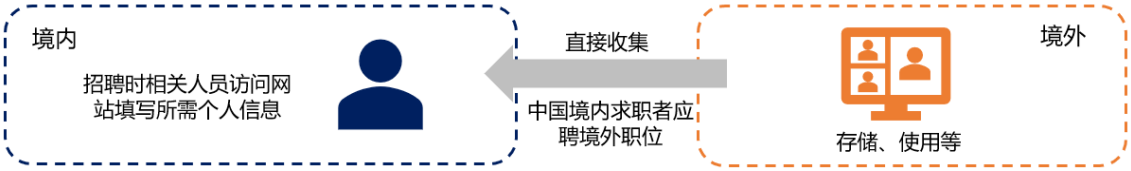


图 10

b) **境内企业将境内收集的招聘相关个人信息上传至境内服务器，由境外母公司直接访问、调取境内服务器上的数据（图 11）**

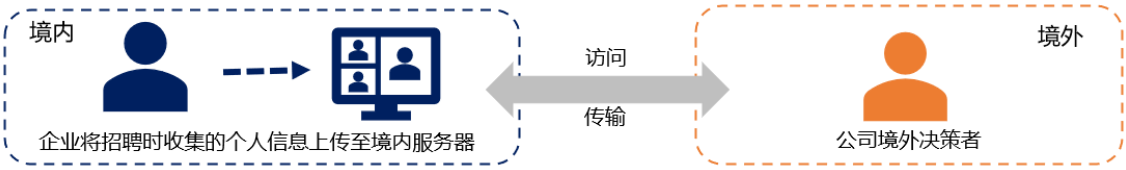


图 11

c) **境内企业聘请第三方机构收集候选人信息，并由第三方机构将收集的数据同步传输至境外（图 12）**

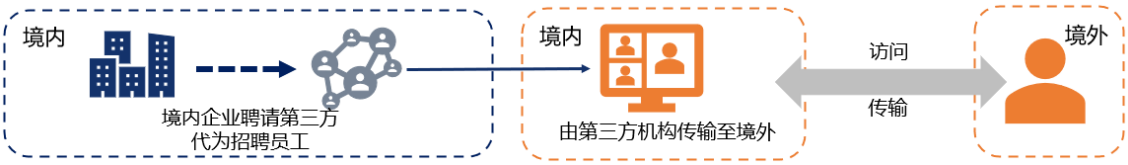


图 12

此外，值得注意的是，企业在招聘时通常会收集应聘者的姓名、性别、联系方式、学历、工作经验等个人信息。但是，由于企业尚未与应聘者签署劳动合同，所以此时《个人信息保护法》第十三条第一款第二项规定的“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”并不能作为收集个人信息的合法性依据。因此，在这种情形下，处理个人信息

的合法性基础为《个人信息保护法》第十三条第一款第一项下的“取得个人的同意”。企业应首先告知应聘者处理其个人信息的目的，并在依法获得个人信息主体的明确授权（包括单独同意）后，方可进行收集、向境外提供个人信息等一系列处理活动。

2. 员工数据出境

在公司人力资源管理的过程中，可能被认定涉及数据出境的典型场景如下：

a) HR 等相关人员通过邮件或特定形式定期向境外主体传输员工数据（图 13）

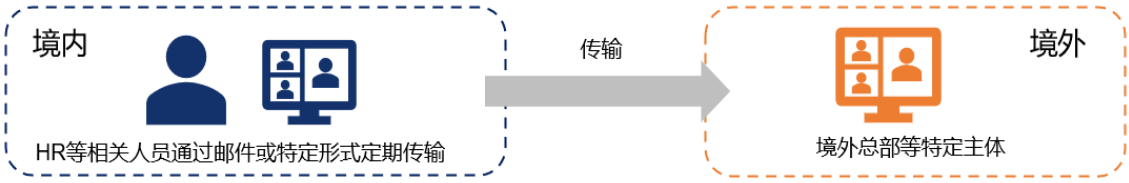


图 13

b) 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该境内系统（图 14）

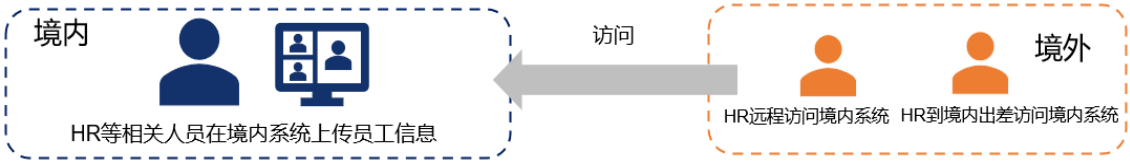


图 14

c) 境外主体直接通过全球人力资源管理系统收集境内员工数据（图 15）

图 15

3. 业务数据出境场景

业务活动开展过程中可能涉及的数据出境场景主要包括三种：一是境内企业通过 ToB 和 ToC 业务收集用户个人信息，并将个人信息传输至境外或者允许境外访问存储在境内的数据；二是企业应境外总部要求将自身运营过程中产生的数据（比如生产、技术、经营业务数据、重要/核心数据等）直接存储在部署于海外的服务器上，或者存储在境内服务器上但允许境外主体查询、调取、下载、导出存储于境内服务器的上述数据；三是设立在中国境外的企业直接收集境内用户的个人信息（如图 16）。

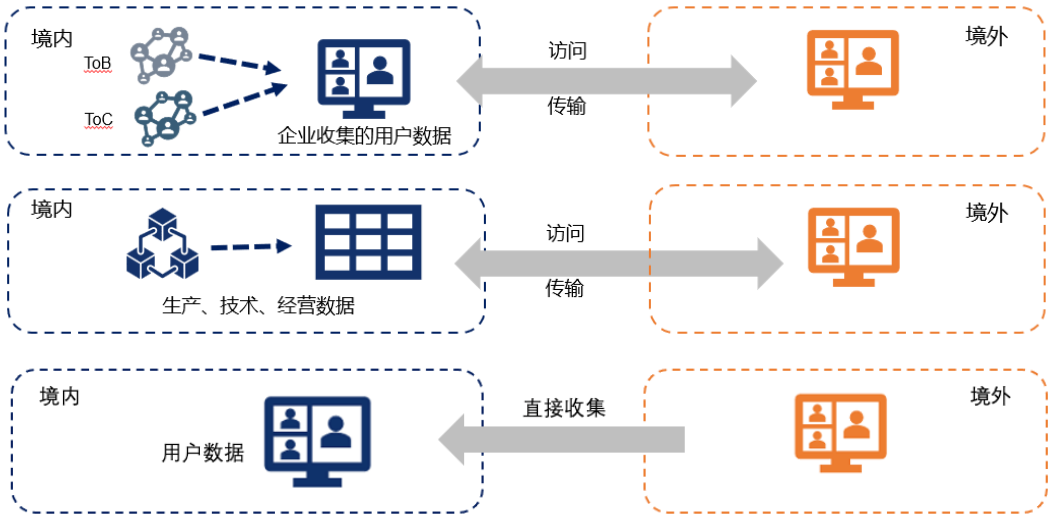


图 16

值得注意的是，在以上场景中，企业均有可能引入第三方供应商并委托其处理数据（比如引入薪酬管理机构处理员工个人信息），此时企业仍是跨境传输场景中的数据处理者/数据提供方，而供应商仅为受托方或技术提供方。

二十四、 如何准确识别跨境传输数据的类型？

在实践中，企业往往会遇到难以识别个人信息、敏感个人信息、重要数据的问题。

（一）个人信息的识别

《个人信息保护法》与《网络安全法》均明确了个人信息的概念，其判断

的标准主要在于信息是否“已识别”或“可识别”自然人个人身份。但是，经过匿名化处理过的信息则不属于个人信息[17]。

企业通常对个人信息进行去标识化或匿名化处理。需要注意的是，虽然经匿名化处理的个人信息因无法再识别到个人而不再是个人信息，但是经去标识化处理的个人信息若在借助额外信息的情况下可以再次识别到个人，则仍属于个人信息。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对这些字段进行了保留。在这种情况下，即使出境方企业在本次数据传输中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 映射的方式将这些信息识别到具体个人。此时，出境后的数据依然保留了个人信息的属性，应当被认为属于个人信息出境。

（二）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[18]。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。GB/T 35273-2020《信息安全技术 个人信息安全规范》在附录 B 列举了部分敏感个人信息类型，为企业合规实践提供了指引。

但是，在实践中，许多企业对经过去标识化处理后的敏感个人信息是否还应被视为敏感个人信息存在疑问。根据向省级网信办等监管部门咨询的结果，如果去标识化处理能够改变敏感个人信息的性质，那么经该等处理后的个人信息不再属于敏感个人信息。换言之，如果经过去标识化处理的敏感个人信息被泄露或者非法使用，且泄露和非法使用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，那么经过去标识化处理的“敏感个人信息”不再属于敏感个人信息。

（三）重要数据的识别

（具体内容请见《上篇：基础篇》“十五、识别重要数据的法律法规依据有

[17] 《个人信息保护法》第四条；《网络安全法》第七十六条。
[18] 《个人信息保护法》第二十八条。

哪些？”部分）

二十五、 如何正确盘点跨境传输数据的数量？

在盘点跨境传输数据的数量时，企业可关注以下要点：

（一）在空间维度方面

在《跨境流动规定》发布实施前，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。

但根据《跨境流动规定》第七条第二款和第八条第二款以及《<促进和规范数据跨境流动规定>答记者问》可推知，目前企业在统计跨境传输数据的数量是否达到适用数据出境制度的门槛条件前，应先评估是否属于《跨境流动规定》提出的豁免情形，即（1）国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的不含个人信息和重要数据的数据向境外提供；（2）境外个人信息在我国处理且没有境内个人信息或者重要数据参与时，其后续向境外提供；（3）为订立、履行个人作为一方当事人的合同确需向境外提供个人信息；（4）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跨境人力资源管理确需向境外提供员工个人信息；（5）紧急情况下为保护自然人的生命健康和财产安全确需向境外提供个人信息；（6）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息且不含敏感个人信息；（7）自由贸易试验区内数据处理者向境外提供负面清单外的数据。如果属于以上除了第（6）项以外的豁免情形，则不需要再计入累计数量。

同时，《<促进和规范数据跨境流动规定>答记者问》《数据出境安全评估申报书（模板）》等进一步明确：（i）在盘点跨境传输的个人信息数量时，应**以自然人为单位去重后的统计结果为准**；（ii）对于**境外接收方数量众多、范围不确**

定、无法逐一列举的，可以在申报时提供**统计数据**（关于此项要求的实际操作方式还有待监管部门提供更为详细的解释说明）。

此外，统计跨境数据数量时，除从境内传输数据至境外这一场景，境外访问境内运营中收集的数据也属于数据跨境传输的场景之一（具体内容请见《下篇：实践篇》“一、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的数据总量中。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。数据出境申报者可以考虑通过网络流量监测的方式，对数据出境行为进行检测，检测、记录跨境数据传输的方式、跨境数据传输目的 IP、通过 IP 地址库识别从境内传输数据至境外或境外访问境内数据的数量。根据咨询监管机构的结果，境外数据处理者访问境内数据这一情形的数据数量应以境外处理者可访问的数据数量计算。

（二）在时间维度方面

《评估办法》和《标准合同办法》在计算出境数据数量时以“自上年 1 月 1 日起”为计算起始时间点，统计企业自上年 1 月 1 日起累计向境外提供的个人信息/敏感个人信息数量。《跨境流动规定》发布实施后，不再谈论上一年度累计个人信息出境数量问题，而是以“当年 1 月 1 日”起为基准、计算至申报数据出境安全评估之日。虽然两种统计方式都是以企业历史以往对外传输数据量为判断标准，但后者缩短了计算出境数据数量的时间周期，一定程度上提高了适用数据出境制度的门槛条件。

此外，需要注意的是，《数据出境风险自评估报告（模板）》还要求涉及个人信息出境的数据处理者，不仅需要在自评估报告中按照自然人（去重）统计**当年的出境数量**，还需**预估未来 3 年的出境数量**。

二十六、 如何确定落实数据跨境传输合规措施的内部牵头部门？

企业在落实数据跨境传输合规措施时，可能会需要法务、信息安全与安全运维、审计内控、人力资源等多个部门联动配合。

其中，法务部门通常负责协助相关部门识别在业务开展过程中涉及的各种数据类型，梳理各种类型数据的境内外传输链路，确定企业与合作伙伴、供应商等不同角色间的数据处理关系（如委托处理或者共享）等工作。信息安全与安全运维部门通常负责梳理数据出境安全操作流程、建立数据安全管理制度以及制定数据出境安全事件应急预案、安排相关应急演练等工作。审计内控部门通常负责对上述部门制定的数据出境相关安全策略、管理制度、出境操作流程以及安全措施等的充分性和有效性进行审计工作。此外，根据数据出境场景的差异，数据出境合规工作也可能会需要人力资源部门或其他业务部门的参与和配合。

因此，企业在开展数据跨境传输合规工作时可以决定由某特定部门/团队担任牵头部门的角色。由于牵头部门需要制定和实施有效的数据跨境传输合规措施并对各相关部门进行统筹协调，故该部门应具备足够的专业能力和资源，包括法律、技术、风险管理等方面的专业知识和综合经验。实践中，一般由企业的法务部门担任牵头部门的角色，并聘请第三方咨询机构（如律所等）进行协助并提供建议，确保数据出境各环节合法合规。

二十七、 如何确定数据出境安全评估的申报主体？

根据《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。

值得注意的是，根据《评估申报指南（第二版）》和《标准合同备案指南（第二版）》规定，未在中国境内设立办事机构或分支机构的境外主体如果向境内自然人提供产品服务，构成在境外处理中国境内自然人个人信息的情况，那么当其符合法定需要申报数据出境安全评估的情形时，也应遵守《评估办法》的规定。考虑到《个人信息保护法》第五十三条提出，“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，对于数据处理者从境外直接获取境内的重要数据和个人信息且达到申报标准的情况，该数据处理者应由国内指定机构代其进行申报。

此外，在实践中，企业通常会委托第三方供应商代为处理企业数据，并认为可以由该供应商代为申报数据出境安全评估。但对此不可一概而论—若第三方供应商仅按照企业委托的数据处理目的和数据处理范围进行数据处理，则第三方供应商在此时承担“代理人”而不是数据处理者的角色，因此不能担任数据出境安全评估的申报主体。

二十八、 如何把握数据出境安全评估的申报时间？

考虑到申报数据出境安全评估提交材料的多样性以及整体申报流程的复杂性，企业在规划数据出境安全评估申报的时间表时，应当为材料准备阶段以及材料审核阶段预留出充分的时间。

首先，企业应当为开展自评估和合规整改工作预留出充分的时间。在数据出境安全评估的申报过程中，企业往往需要提交一系列材料，包括数据出境风险自评估报告、数据出境安全评估申报书以及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等[19]。考虑到数据出境风险自评估工作往往会涉及多个部门的协调沟通并且需要进行一定程度的合规整改（如完善公司内部制度或者对已签署的数据处理协议进行修订等），所以企业无论是自行还是委托第三方机构开展数据出境风险自评估工作都需要耗费大量的时间，需要根据自身的数据合规情况为此部分的准备工作提前做好时间上的安排。但是，同时提示企业注意，数据出境风险自评估活动应当在数据出境安全评估申报前 3 个月内完成[20]。所以，提前部署数据出境安全合规工作的企业在提交申报之前还需要关注自评估活动的完成日期，如果自评估报告的完成时间距离提交数据出境安全评估申报的时间已经超过 3 个月，还应重新进行自评估并更新报告的内容。

[19] 《评估办法》第六条；《评估申报指南（第二版）》第三条。
[20] 《评估申报指南（第二版）》附件 4《数据出境风险自评估报告（模版）》。

其次，企业也应为材料提交后的审查阶段预留出充分的时间。如前文所述，数据出境安全评估申报的整体时长为 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（具体内容请见《上篇：基础篇》“六、数据出境安全评估的流程是怎样的？”部分）。在实际申报中，企业可能需要根据网信部门的要求多次对申报材料进行修改、完善以及补充。由于法律法规未对补充材料审核期限（即上述 57+N/72+N 天中的 N 天）作出限制，所以申报实际所需的时间可能远超过 57 天或者 72 天。

因此，有需求的企业应提前对数据出境安全评估申报进行规划，综合考虑自身开展自评估和合规整改工作可能耗费的时长并预留网信办审查阶段的时间，避免因数据出境安全评估申报的原因耽误数据出境相关业务的合法合规开展。

二十九、 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？

根据《评估申报指南（第二版）》的规定，适用线上申报方式的数据处理者应当通过数据出境申报系统提交材料；而适用线下方式进行申报的数据处理者应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。（具体内容请见《上篇：基础篇》“六、数据出境安全评估的流程是怎样的？”部分）

我们同时以附件的方式列明了国家及各地省级网信部门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要求。（具体内容请见“附件一、国家及各地省级网信部门联系方式”部分）

三十、 如何开展个人信息保护影响评估？

在跨境传输数据之前，企业需要根据自身业务情况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合法合规至关重要。

出境合规流程的第一步是开展个人信息保护影响评估（下称 **PIA**），自行组

织评估数据出境的安全风险。根据《个人信息保护法》第五十五条的规定，企业作为个人信息处理者，只要存在“向境外提供个人信息”的情况就应当事前进行 PIA，《标准合同办法》第五条也重申了这一要求。同时，《标准合同办法》第七条规定，如果企业以个人信息出境标准合同作为个人信息出境的合规路径，则需要同步提交 PIA 报告。《标准合同备案指南（第二版）》附件 3 进一步要求企业提交的 PIA 报告应当在个人信息出境标准合同备案之日前 3 个月内完成，且至备案之日未发生重大变化。

综合来看，企业应参考《个人信息保护法》第五十六条、GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》《标准合同办法》以及《标准合同备案指南（第二版）》的相应内容准备 PIA 报告。其中，《标准合同备案指南（第二版）》附件 5《个人信息保护影响评估报告（模板）》明确规定，用于个人信息出境标准合同备案的 PIA 报告应严格按照模板撰写，具体包含以下内容：

1. 出境活动整体情况：

   - 个人信息处理者基本情况，包括个人信息处理者基本情况简介、整体业务与处理个人信息情况、拟出境个人信息情况以及遵守个人信息保护相关法律法规的情况；
   - 境外接收方情况，包括境外接收方基本情况、境外接收方处理个人信息的用途和方式、境外接收方履行责任义务的管理和技术措施、能力等；
   - 个人信息处理者认为需要说明的其他情况。

2. 拟出境活动的影响评估情况及结论：

   根据《标准合同办法》第五条规定的以下评估事项，说明个人信息保护影响评估情况，**重点说明评估发现的问题和整改情况**，并对个人信息出境活动作出客观的影响评估结论，充分说明得出评估结论的理由和论据：

   - 个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；

- 出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；
- 境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；
- 个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
- 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对标准合同履行的影响；
- 其他可能影响个人信息出境安全的事项。

三十一、 如何开展数据出境风险自评估？

除 PIA 之外，当企业符合需要向网信部门申报数据出境安全评估的情形时，企业还应当组织开展数据出境风险自评估，作为申报的前置程序。

《评估申报指南（第二版）》附件 4《数据出境风险自评估报告（模版）》明确规定自评估报告应当严格按照模版撰写，包含以下内容：

1. 自评估工作情况；
2. 出境活动整体情况：
   - 数据处理者基本情况，包括基本情况简介、组织架构和数据安全管理机构信息、整体业务与数据资产情况；
   - 拟出境数据情况，包括①数据出境涉及业务、数据资产等情况、②数据出境及境外接收方处理数据的目的、范围、方式，及其合法性、正当性、必要性、③按照申报业务场景梳理对应的出境数据项情况、④拟出境数据在境内存储的系统平台、数据中心（包含云服务）等情况，数据出境链路相关情况，计划出境后存储的系统平台、数据中心等、⑤数据出境后向境外其他接收方提供的情况、⑥涉及个人

信息的，按照自然人（去重）统计当年的出境数量，预估未来 3 年的出境数量；

- 数据处理者数据安全保障能力情况，包括数据安全管理能力、数据安全技术能力、数据安全保障措施有效性证明、遵守数据和网络安全相关法律法规的情况；
- 境外接收方情况，包括境外接收方基本情况、境外接收方处理数据的用途、方式等、境外接收方履行责任义务的管理和技术措施、能力等；
- 法律文件约定数据安全保护责任义务的情况，包括①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、②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、③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、④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、⑤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、⑥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；
- 数据处理者认为需要说明的其他情况。

3. 出境活动的风险自评估情况及结论：

对照《评估办法》第五条规定的如下评估事项，说明数据出境风险自评估情况，**重点说明自评估发现的问题和整改情况**，对拟申报的数据出境活动作出客观的风险自评估结论，充分说明得出自评估结论的理由：

- 数据出境和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；

- 出境数据的规模、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；
- 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；
- 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
- 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等是否充分约定了数据安全保护责任义务；
- 其他可能影响数据出境安全的事项。

三十二、 数据跨境传输场景下的 PIA 与数据出境风险自评估是一回事吗？

PIA 与数据出境风险自评估并不相同。PIA 是《个人信息保护法》第五十五条明确提出要求企业在向境外提供个人信息前应当开展的自评估工作，而数据出境风险自评估则是《评估办法》第五条提出的要求符合数据出境安全评估申报情形的企业在申报前应当开展的自评估工作。

换言之，如果企业拟向境外提供个人信息尚未达到《评估办法》和《跨境流动规定》规定的申报门槛，则企业仅需要完成 PIA，并在准备采取相应的数据出境制度（如签订和备案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。但是，如果企业符合须开展数据出境安全评估申报的情形（具体内容请见《上篇：基础篇》“五、哪些情况下需要申报数据出境安全评估？”部分），企业除开展 PIA 之外还需要进行数据出境风险自评估。

将 PIA 的评估事项与数据出境风险自评估进行比较可以发现，这两者存在一定的异同。

PIA	数据出境风险自评估
《个人信息保护法》第五十六条： 个人信息保护影响评估应当包括下列内容： （一）个人信息的处理目的、处理方式等是否合法、正当、必要； （二）对个人权益的影响及安全风险；（三）所采取的保护措施是否合法、有效并与风险程度相适应。	**《评估办法》第五条：** 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，重点评估以下事项： （一）数据出境和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； （二）出境数据的规模、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； （三）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； （四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等； （五）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等是否充分约定了数据安全保护责任义务； （六）其他可能影响数据出境安全的事项。

从关注重点来看，PIA 落脚于保障个人信息主体权益，包括个人信息处理活动是否正当、合法、必要以及是否采取了安全保护措施等。而数据出境风险自评估则更注重数据出境活动对国家安全、公共利益、个人或组织合法权益带来的风险。

从内容上讲，数据出境风险自评估的范围大于 PIA。数据风险自评估除包括了 PIA 的评估内容，还增加了判断数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务等内容。

总体而言，在个人信息出境场景下，尽管数据出境风险自评估与 PIA 报告的关注点有所不同，但是两者的目标和基本评估内容是相近的，都需要对个人信息出境活动进行分析和评估，筛选出潜在的漏洞和风险，并判断所采取的保护措施是否能够保证个人信息的安全。

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可以在 PIA 内容的基础上进一步补充评估、完成数据出境风险自评估要求。但需要注意，《评估申报指南（第二版）》要求数据出境风险自评估报告严格按照模板撰写，所以企业在基于 PIA 内容补充评估时，应同时确保对标模板要求产出自评估报告。另外，PIA 报告和处理情况记录应当至少保存三年。如果企业将 PIA 报告和数据出境风险自评估报告合并完成，则需要将该报告至少保存三年。

三十三、 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？

根据《评估办法》第五条以及《评估申报指南（第二版）》附件 4《数据出境风险自评估报告（模版）》，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，除了评估数据处理者自身的数据安全保障能力以外，还应将境外接收方“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”也列为重点评估事项。由此可见，正确对数据安全保障能力进行评估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。以下我们将以评估数据处理者的数据安全保障能力为例详细展开介绍。

《评估申报指南（第二版）》附件 4《数据出境风险自评估报告（模版）》中列举了评估数据处理者的数据安全保障能力所应包含的内容：

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（涉及个人信息出境的，需额外向网信办提供履行《个人信息保护法》第三十九条规定的情况说明及佐证材料，包括**告知义务和取得个人的单独同意**等，若企业在拥有《个人信息保护法》下豁免同意场景涉及的合法基础的前提下，**不需取得个人同意**）；

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（如涉及受到行政处罚和监管整改的，可额外向网信办提供证明整改完成的相关佐证材料）。

对于以上评估内容，根据与监管机构的咨询来看，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，上述内容也均需要在企业提交的《数据出境风险自评估报告》中有所体现。监管机构表示企业提交的总结评估的内容越详细，越有助于监管机构正确评价企业的数据安全保障能力。

在实践中，一般着重从管理制度保障能力与技术手段保障能力两个方面对企业的“数据安全保障能力”进行评估：

（一）管理制度保障能力

企业应当根据相关法律法规详细描述数据安全有关的管理组织体系和制度建设情况[21]，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[22]。一般来说，此部分的安全保障能力评估工作需要法务、安全、技术、审计等部门共同协作完成。

[21] 包括但不限于《数据安全法》《网安条例（征）》《评估办法》《评估申报指南（第二版）》。
[22] 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

（二）技术手段保障能力

企业应当具备总体安全防护技术手段和数据安全技术防护体系以保障所传输数据的保密性、完整性和可用性。

企业应在评估事项中详细描述所采取的安全措施、所具备的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以及对数据发送、传输、销毁等各阶段进行审计的能力等[23]。由于简单的书面文件审查无法对上述技术手段进行全方面的测评，建议企业在实际开展自评估时咨询相关领域技术专家的意见，对技术手段保障能力进行充分的评估并获取专业意见。

除这两方面的评估说明外，企业仍需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[24]，进一步证实其整体的数据安全保障能力。

根据咨询监管机构的结果，企业在对境外接收方的数据安全保障能力进行评估时应与对数据处理者的数据安全保障能力进行评估时的维度一致，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。

三十四、 如何评估境外接收方法律与政策环境完善程度？

尽管根据网信办发布的《数据出境风险自评估报告（模板）》《个人信息保护影响评估报告（模板）》，企业已无需在进行数据出境风险自评估或 PIA 时评估境外接收方所在国家或地区个人信息保护政策法规情况，减轻了企业所需承担的合规负担。但需要注意的是，即使企业无需在数据出境风险自评估报告或备案的 PIA 报告中说明此项内容，根据国家网信办制定的《个人信息出境标准

[23] 具体合规义务可参考《评估办法》《评估申报指南（第二版）》。
[24]《评估申报指南（第二版）》附件 4《数据出境风险自评估报告（模板）》。

合同》第四条的要求，企业仍应评估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是否会影响其履行合同约定的义务，并记录评估过程与结果。同时，《评估办法》第八条要求网信部门在进行数据出境安全评估时，应考虑“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”。由此可以看出，境外接收方法律与政策环境完善程度仍是值得企业关注的风险评估项。故建议企业在向境外提供数据前，事先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。

根据《评估办法》《认证规范 V2.0》《安全评估指南（征）》《跨境认证要求（征）》等规定，在评估境外接收方法律与政策环境完善程度时应包含以下几项内容：

1. 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；

2. 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；

3. 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，具体包括：

   - 境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生数据安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况；

   - 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；

   - 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；

   - 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。

4. 针对重要数据境外接收方所在国家或者地区的法律与政策环境，可评估：

- 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；
- 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；
- 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；
- 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则可参考下表标准[25]：

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。

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

[25] 《安全评估指南（征）》附录 B.3.3.1。

策环境保障能力则可参考下表标准[26]：

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。

同时，由于对境外接收方法律政策环境进行评估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，企业需要与境外接收方密切联系，并建议聘请律师或其他跨国服务机构协助，以实现全面、深入的有效评估。

三十五、 欧盟是如何对法律政策环境进行评估的？

我国对于如何评估数据接收方所在法律政策环境尚无明确详细的指引，故在实践中，为了进一步提升合规水平，企业也可同步参考在数据隐私保护法治方面领先的欧盟标准。

在欧盟法院于 2020 年 7 月作出 Schrems II 案件的判决后[27]，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**）

[26] 《安全评估指南（征）》附录 B.3.3.2。
[27] 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。

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）[28]，就开展数据跨境传输评估（**DTIA**）提供指引，尤其强调要对第三国的数据保护法律或实践进行评估。

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”，要求相关方必须遵守该等四项保障以确保对隐私权和个人数据的保护符合欧盟法院及欧洲人权法院的判例所要求的标准。当数据提供方评估第三方国家是否具备与欧盟基本相同的数据保护标准时，数据提供方应评估第三方国家赋予政府访问和要求披露数据的权力的法律是否满足上述“欧盟重要保障”要求，具体包括：

1. 应当基于清晰、准确和公开的规则处理数据：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. 所采取的措施必须是为了达到合理目的必要且适当的，并需要说明该措施的必要性和适当性：此处特别强调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且适当；

3. 应当具备独立的监督机制；

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。

2023 年 7 月 10 日，欧盟委员会通过了《欧盟-美国数据隐私框架》(EU-U.S. Data Privacy Framework)的充分性决定。该决定认可参与《欧盟-美国数据隐私框架》的美国公司可以提供与欧盟相当的数据保护水平。根据新的充分性决定，个人数据可以安全地从欧盟流向获得《欧盟-美国数据隐私框架》认证的美国公

[28] 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）。

司，而无需实施额外的数据保护保障措施或进一步授权。

综合前述我国及欧盟法律法规的规定，企业在评估境外接收方所在国家或区域的法律与政策环境时可以重点考虑对以下方面进行评估：

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；

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、所作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[29]；

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[30]。

[29] 参见《认证规范 V2.0》第 5.4 条 e) 1)项。
[30] 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。

三十六、 数据出境安全评估的有效期为多久？什么情况下需要再次申请安全评估？

《跨境流动规定》第九条对数据出境安全评估结果的有效期进行了调整，从原先《评估办法》规定的 2 年延长至 3 年，并从评估结果出具之日起开始计算。此外，《跨境流动规定》增加了数据处理者申请延长评估结果有效期的规定。若数据处理者在有效期满后仍需继续开展数据出境活动，且未出现需要重新进行出境安全评估的情况，数据处理者可以在有效期届满前的 60 个工作日内，通过所在地的省级网信部门向国家网信部门提交延长评估结果有效期的申请。经国家网信部门的批准，评估结果的有效期将可再延长 3 年。

此外，《评估办法》第十四条同时规定，在数据出境安全评估的结果有效期内出现以下情形之一的，数据处理者应当重新申报评估：

1. 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；
2. 境外接收方所在国家或者地区数据安全保护政策和网络安全环境发生变化以及发生其他不可抗力情形、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法律文件变更等影响数据出境安全的；
3. 出现影响数据出境安全的其他情形。

三十七、 什么情况下需要重新签署个人信息出境标准合同并履行备案手续？

《标准合同办法》第八条和《标准合同备案指南（第二版）》规定了补充或者重新订立标准合同并履行备案手续的情形，包括：

1. 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；

2. 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；

3. 可能影响个人信息权益的其他情形。

值得注意的是，当出现上述情形时，个人信息处理者除需要补充或者重新订立标准合同并备案外，还应当重新开展 PIA 并出具相应报告。

三十八、 在订立监管机构发布的标准合同时是否可以对内容进行修改？

《标准合同办法》第六条明确规定“标准合同应当严格按照本办法附件订立。国家网信部门可以根据实际情况对附件进行调整。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。”

因此，企业应严格按照网信部门提供的模板订立标准合同，不得对其作出修改。但是，企业可以在标准合同附件中补充关于个人信息出境场景的具体信息。国家网信办发布的《个人信息出境标准合同》也设置了“附录二、双方约定的其他条款”这一模块，允许双方以附录的形式，在与标准合同不相冲突的前提下，约定其他条款安排。

但是，企业需注意由于这些新增条款不得与标准合同条款相冲突，所以新增条款仅能起到“补充”作用（如对境外接收方采取的管理和技术措施细节等方面作出具体约定等），不能对标准合同条款进行实质性调整（如不得削减个人信息主体的权益或者减少个人信息处理者/境外接收方的责任和义务等）。

我们同时以附件的方式列明了国家及各地省级网信部门联系方式，便于企业结合自身实际业务情况了解个人信息出境标准合同备案工作的最新相关要求。（具体内容请见“附件一、国家及各地省级网信部门联系方式”部分）

三十九、 如果已与境外接收方签署《数据处理协议》，是否可将标准合同作为其附件？

企业如果选择以订立并备案《个人信息出境标准合同》作为个人信息出境活动的合规路径，那么即便已经与境外接收方签署《数据处理协议》，也不能免除企业《个人信息出境标准合同》的相关义务，其仍然应当严格按照国家网信办发布的《个人信息出境标准合同》与境外接收方订立标准合同，并将签署生效后的标准合同通过数据出境申报系统备案。但是，企业可以将标准合同作为《数据处理协议》的附件，作为网信办审查的辅助性支持材料。

如果在形式上存在任何疑问，企业也可以通过“附件一、国家及各地省级网信部门联系方式”与相关网信部门沟通，根据自身情况确认个人信息出境标准合同备案工作的具体要求。

四十、 企业应当向哪个/些机构申请个人信息保护认证？

《认证公告》指出“从事个人信息保护认证工作的认证机构应当经批准后开展有关认证活动”。但是，相关法律法规并未明确公布依法取得认证机构资质的企业名录。

中国网络安全审查认证和市场监管大数据中心在其官方网站发布公告[31]，即“网安审认证和市监大数据中心负责个人信息保护认证的具体实施工作”。网安审认证和市监大数据中心还在网站上发布了个人信息保护认证申请书模版，并上线了可办理个人信息保护认证业务的“数据安全认证业务管理系统”（https://data.isccc.gov.cn）。根据向网安审认证和市监大数据中心咨询的结果以及国家网信办于 2024 年 3 月 22 日发布的《<促进和规范数据跨境流动规定>答记者问》，企业在跨境传输个人信息时可以选择通过“数据安全认证业务管理系统”中的“个人信息保护认证管理系统”向网安审认证和市监大数据中心申请进行个人信息保护认证。

[31] https://www.isccc.gov.cn/zxyw/sjaq/grxxbhrz/index.shtml，访问日期 2024 年 3 月 23 日。

四十一、 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？

在涉及国际争议时，难免会发生境外司法机构要求境内企业向其提供企业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。

根据《数据安全法》第三十六条和《个人信息保护法》第四十一条的规定，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。

对此，应由主管机关依据有关法律、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外国司法或者执法机构关于提供存储于境内数据或个人信息的请求。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 86 项中外双边司法协助条约的规定开展，或在司法途径不适用的情形下，由外交部通过外交途径开展。

然而近些年来，在实践中较为常见的是企业在境外的民事纠纷诉讼过程中，外国法院或其他司法机构未通过司法途径或外交途径，而是直接要求企业将其在境内的相关数据信息作为证据材料提交。根据司法部司法协助中心对于相关咨询问题的答复，无论是企业应境外司法机构的要求被动提交证据，还是企业主动向境外司法机构提供证据，均需要向司法部司法协助中心申请批准。具体流程如下：

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。

（注：自评估报告与法律评估报告均需明确所提交证据不包含国家秘密、所涉及商业秘密的部分已做遮挡处理、涉及个人信息的内容已取得个人单独同意。）

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、提交申请的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 1-2 个月，涉及重大复杂的案件则为 2-4 个月。审核通过后，将会为提交申请的企业出具批文，企业可以据此办理证据出境事宜。因此，企业在面临上述情形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，并按要求准备材料、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审批过程中出现的其他问题导致无法按时提交证据的情况发生。截至目前，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。

随着中国对于数据安全的保护力度不断增强，各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。例如，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，这有助于节省企业的成本、提高数据作为证据的跨境流通效率。实践中，我们也建议企业根据个案情况及时评估确定主管机关、尽早联系主管机关进行提交材料、流程、时限等问题的确认以便依据最新监管要求统筹安排。

四十二、 我国粤港澳大湾区个人信息出境标准合同如何签署和备案？

《大湾区标准合同》是注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，或者香港特别行政区的个人信息处理者（就内地而言，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人；就香港特别行政区而言，亦涵盖“资料使用者”，即就个人资料而言，指独自或联同其他人或与其他人共同控制该资料的收集、持有、处理或使用的人）及接收方（指自个人信息处理者处跨境接收个人信息的组织、个人）在进行个人信息跨境流动时订立的合同。《大湾区标准合同》主要内容包括双方的合同义务和责任、个人信息主体的权利和相关的救济方法，以及合同解除、违约责任、争议解决等事项。

个人信息处理者通过订立《大湾区标准合同》跨境提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：

（一）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性；

（二）对个人信息主体权益的影响及安全风险；

（三）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。

个人信息处理者可以与接收方约定其他条款，但不得与《大湾区标准合同》相冲突。跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化，延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当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，并履行相应备案手续。

订立《大湾区标准合同》并生效后，个人信息处理者及接收方即可开展个人信息跨境活动。在合同生效之日起10个工作日内，个人信息处理者及接收方应按照属地分别向广东省互联网信息办公室和政府资讯科技总监办公室进行备案，提交备案所需文件。实践中，广东省网信办不直接接收备案材料，个人信息处理者及接收方应先将备案材料电子版（正式扫描件PDF版和WORD版，

光盘）提交所在地级以上市互联网信息办公室，经材料完整性检查后，由所在地级以上市互联网信息办公室送广东省互联网信息办公室预审。电子版材料预审通过后，个人信息处理者及接收方送达纸质版材料（装订完整）并附带电子版材料（光盘）至广东省互联网信息办公室，电子版材料应当提供与纸质版材料一致的PDF扫描件和WORD版。广东省互联网信息办公室收到材料后，将按备案流程进行处理。

《大湾区标准合同》备案流程包括文件提交、检查文件及回复备案结果、补充或者重新备案等。备案文件包括：法定代表人身份证明文件影印本；承诺书；及签署版的《大湾区标准合同》。个人信息保护影响评估工作必须在《大湾区标准合同》备案之日前3个月内完成，且至备案之日未发生重大变化。与内地标准合同的备案要求相比，个人信息保护影响评估工作报告不需要提交备案。

广东省互联网信息办公室在收到纸质版材料后的10个工作日内完成材料查验，并通知个人信息处理者备案结果。备案结果分为通过、不通过。通过备案的，广东省互联网信息办公室向个人信息处理者发放备案编号；不通过备案的，个人信息处理者将收到备案未成功通知及原因，要求补充完善材料的，个人信息处理者应当补充完善材料并于10个工作日内再次提交。

跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化，延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立大湾区标准合同，并履行相应备案手续。

个人信息处理者在标准合同有效期内补充订立大湾区标准合同的，应当提交补充材料；重新订立大湾区标准合同的，应当重新备案。补充或者重新备案的材料查验时间为10个工作日。

四十三、 上海自贸区有无数据及个人信息出境的便利监管措施？

基于《跨境流动规定》第六条的规定，自由贸易试验区可自行制定需要纳入数据出境程序管理范围的负面清单，且在负面清单以外的数据跨境传输可以

豁免数据出境程序。

上海自贸区即存在相关的数据出境便利政策，其主要基于《上海市落实〈全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案〉的实施方案》（沪府发〔2024〕1号，2024年02月03日生效，“实施方案”）及《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》（沪自贸临管规范〔2024〕3号，2024年02月08日）。

如前述，《跨境流动规定》提出了自贸区负面清单模式：自由贸易试验区在国家数据分类分级保护制度框架下，自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（以下简称负面清单），经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

实施方案提出上海自贸试验区管委会、临港新片区管委会按照数据分类分级保护制度，根据区内实际需求率先制定重要数据目录；并通过在临港新片区建立数据跨境服务中心等，便利数据处理者开展数据出境自评等数据出境安全合规工作。

《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》（“临港办法”）适用于在临港新片区范围内登记注册的，或在临港新片区开展数据跨境流动相关活动的企业、事业单位、机构协会和组织等数据处理者。结合上海“五个中心”建设，围绕汽车、金融、航运、生物医药等重点领域以及临港新片区相关行业的发展要求，以跨境需求最迫切的典型场景为切入口，对跨境数据进行分类管理。临港办法将跨境数据分三级并细化了其数据出境监管要求：

（1）核心数据，是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。核心数据禁止跨

境。（2）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（仅影响组织自身或公民个体的数据，一般不作为重要数据）。数据处理者对重要数据目录内的数据，可通过临港新片区数据跨境服务中心申报数据出境安全评估。（3）一般数据，是指核心数据、重要数据外的其他数据。数据处理者对在一般数据清单内的数据，可向临港新片区管委会申请登记备案，并在满足相关管理要求下自由流动。

前述重要数据目录及纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单等由临港新片区管委会负责制定，并报相关部门批准、备案及后续更新和告知。根据上海市政府新闻办举办多部门参与的新闻发布会记者问答，临港新片区将按照“从企业到行业、从案例到清单、从正面到负面”的原则，率先围绕智能网联汽车、金融理财、高端航运等重点领域，开展一般数据清单和重要数据目录的编制工作，并将于近日发布部分相关清单。

在本《实务问答》发布之时，我们尚未从公开渠道查询到临港片区的一般数据清单和重要数据目录。不过，据有关消息人士，我们理解在实操中，已有相关先例，由注册于临港片区的企业可在通过该片区内有关数据链路接入“数据海关”后，认定其系在片区开展数据跨境活动，并适用片区数据出境的有关豁免；并在满足特定存档备查措施后即可开展数据出境。

四十四、 银行金融业数据出境有无特别规范需要注意？

银行金融业数据合规除应遵守本《实务问答》前述的各项通用规定外，还应注意中国人民银行等其他机构发布的相关规范。其中与数据出境相关的主要包括《个人金融信息保护技术规范》（JR/T 0171—2020，2020年2月13日实施）、《金融数据安全 数据安全分级指南》（JR/T 0197—2020，2020年9月23日实施）、《金融数据安全 数据生命周期安全规范》（JR/T 0223—2021，2021年4月8日实施）等。

就银行金融业的关键信息基础设施运营者的认定和合规请见《下篇：实践篇》“四十五、证券基金业数据出境有无特别规范需要注意？”部分。

就银行金融业的重要数据，《金融数据安全 数据安全分级指南》给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程。根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别从高到低划分为 5 级、4 级、3 级、2 级、1 级。其中 5 级数据特征包括(1)重要数据，通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用;及（2）数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。

该指南附录 C 还详细解释了银行金融业重要数据的认定，具体包括：（1）宏观特征：可反映不可更改或长时间保持稳定的经济特征、社会特征的数据；（2）海量信息汇聚得到的衍生特征数据：汇聚后覆盖多省份的金融消费者真实交易信息；（3）行业监管机构决策和执法过程中的数据：行政机关、执法机关在履职或执法过程中收集和产生的不涉及国家秘密且未公开的受控数据；及（4）关键信息基础设施网络安全缺陷信息：网络设备、服务器、信息系统等有关漏洞信息。

需注意，上述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。《金融数据安全 数据生命周期安全规范》中提到，银行金融业机构境外分、子公司和分支机构在境外开展业务过程中采集、产生的数据，其安全定级及数据保护工作应按照数据跨境相关要求执行。并强调在我国境内产生的金融数据原则上应在我国境内存储，国家及行业主管部门另有规定的除外。其中在我国境内产生的 5 级数据（包括银行金融业重要数据）应仅在我国境内存储。

尽管按《跨境流动规定》，目前未被主管部门和地区告知或/公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估，但银行金融业机构仍然需要基于前述规定做好其数据的分类分级管理，在可能涉及重要数据级别的数据跨境传输时，采取较为审慎的态度。

个人信息在银行金融一般体现为个人金融信息。《个人金融信息保护技术规

范》中对个人金融信息的定义包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息；并将个人信息分级为三级。就个人金融信息的出境，在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，应满足下列要求：（1）应符合国家法律法规及行业主管部门有关规定；（2）应获得个人金融信息主体明示同意；（3）应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；（4）应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。银行金融业的个人敏感信息目前可参照 GB/T 35273-2020《信息安全技术 个人信息安全规范》附录 B 的规定。其中，银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息等个人财产信息属于个人敏感信息。

银行金融业机构在向境外提供个人信用信息时还应关注《征信管理办法》的相关规定，当符合相关适用条件构成征信机构向境外提供个人信用信息的，应当对境外信息使用者的身份、信息用途开展必要审查，确保出境后的信息被用于跨境贸易和投融资等合理用途，且不危害国家安全。

中国人民银行发布的《中国人民银行业务领域数据安全管理办法（征求意见稿）》中也有关于数据出境限制管理的要求，待该办法正式出台生效后，银行金融机构也应参照执行。

四十五、 证券基金业数据出境有无特别规范需要注意？

证券基金业数据合规除应遵守本《实务问答》前述的各项通用规定外，还应注意中国证券监督管理委员会等其他机构发布的相关规范。其中，与数据出

境相关的主要包括《证券期货业数据分类分级指引》（JR/T 0158—2018，2018年9月27日实施）、《证券期货业数据安全管理与保护指引》(JR/T 0250—2022，2022年11月14日实施)、《证券期货业数据安全风险防控 数据分类分级指引》（GB/T 42775-2023，2023年8月6日实施）等。

就CIIO，证券基金业机构因其与国家经济金融安全的关系，一般被认为易构成关键信息基础设施运营者,但截止本文起草时间，公开渠道尚未发现证券基金业主管部门发布或明确指定的相关关键信息基础设施运营者名单。

就证券基金业的重要数据，《证券期货业数据分类分级指引》发布时间较早，并未明确指明重要数据，和目前重要数据及数据出境的相关规定衔接可能存在一定不确定性。该指引主要根据影响对象（行业、机构、客户）、影响范围（多个行业、行业内多机构、本机构）、数据安全属性（完整性、保密性、可用性）遭到破坏后带来的影响程度（严重、中等、轻微、无）将证券基金业数据划分为四级并就其处理规范提出了要求：4级（极高），数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用；3级（高），数据用于重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用；2级（中），数据用于一般业务使用，一般针对受限对象公开，一般指内部管理且不宜广泛公开的数据；1级（低），数据一般可被公开或可被公众获知、使用。

但在证券基金业的数据出境活动中，还值得关注该指引中提到的因数据聚合、数据时效性导致的分级变更。具体而言数据在流转、传递、使用过程中，因各类业务需要，可能需要将相同或不同级别的数据汇聚在一起进行分析、处理。对该等数据聚合，需注意：（1）因业务需要，将来自不同途径或不同系统的数据汇聚在一起，数据的原始用途或所在系统发生改变，需要对数据进行重新确定类别并定级；（2）需要深入分析汇聚后数据是否可能较原始数据获得更多的信息，并判断汇聚后的数据安全属性（完整性、保密性、可用性）遭到破坏后的影响，以准确定级；（3）汇聚后数据级别一般不低于所汇聚的原始数据的最高级别。同理，还应注意数据时效性对数据分类分级影响。我们认为上述原则在证券基金业重要数据认定及数据出境合规方面有适用的可能性。

《证券期货业数据安全风险防控 数据分类分级指引》基本延续了《证券期货业数据分类分级指引》中关于分级的规定;《证券期货业数据安全管理与保护指引》中主要采取引用的方式，提及向境外提供数据、个人信息的，应依据《网络安全法》等相关法规规定。证券基金业机构在数据出境过程中，还应关注《证券法》和《期货和衍生品法》等相关规定，跨境证券、期货等行业的监督管理应在国务院证券监督管理机构的参与下进行，境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动；且未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动、期货业务活动等有关的文件和资料。

尽管按《跨境流动规定》，目前未被主管部门和地区告知或/公开发布为重要数据的，数据处理者尚可无需作为重要数据申报数据出境安全评估，但证券基金业企业仍应需要基于前述规定做好其数据的分类分级管理，在可能涉及重要数据级别的数据跨境传输时，采取审慎态度。

四十六、 医药行业跨境传输的常见场景有哪些？

在医药行业中，不论是有意于海外市场发展的中资企业，还是深耕中国市场的跨国企业，均广泛地涉及不同场景下的跨境数据传输。这些数据传输广泛存在于从研发到上市、商业化以及跨境许可交易等场景下。

在医药研发过程中，国际多中心临床研究（Multi-regional clinical trials，MRCT）是一个十分常见的场景。在 MRCT 中，不同国家和地区的试验数据往往会基于某一临床试验的方案同时进行临床试验，期间大量的临床数据得以交换和共享，并汇总于医药企业手中。临床数据在这一场景下被广泛采集和传递，除涉及前述的数据及个人信息外，也涉及人类遗传资源信息等性质的数据。此外，在这一场景中，医药企业可能也会聘用电子数据采集（EDC）等第三方服务机构为其提供数据管理等服务，而相关的服务器也可能位于境外。

在向境外的医药监管机构提交如 IND（Investigational New Drug，新药临床试验审批）和 NDA（New Drug Application，新药注册申请）等申报时，也往往

涉及有关数据的跨境传输。比如，在 IND 场景下，境内可能会向境外提交的研究计划和研究方案等资料，在 NDA 场景下，境内可能会向境外提交各项临床数据、病例报告以及有关的统计数据等。

在医药行业的跨境许可交易（License-in/License-out）下，境外引进方可能基于与境内许可方的协议约定，要求境内许可方向其提供相关技术和资料，这其中可能就涉及境内许可方此前已经保存的临床试验数据、资料和报告。

此外，在跨境的学术交流、向境外机构分享/发布相关临床数据的场景中，也可能涉及境内医药行业数据的跨境传输。

四十七、 医药行业跨境传输涉及的数据有哪些类型？

如前所述，医药行业的多种场景下均可能涉及数据的跨境传输。从网信部门的监管角度来看，（考虑到目前实操中大多数企业并未被认定为 CIIO 的前提）医药企业需要厘清相关数据的属性，以便据此结合数量等其他信息判断医药企业需要履行何种合规路径（申报并通过数据出境安全评估、订立并备案个人信息出境标准合同或通过个人信息保护认证）。从部门监管角度来看，也需要根据相关数据的属性以明确其具体所需满足的合规事项。

从数据的监管角度考虑，企业可能需要厘清相关数据是否构成重要数据或核心数据。如前所述，基于《跨境流动规定》第二条的规定，目前以地方和行业主管部门的告知/公开发布为标准，未被告知/公开发布的，则不需要将相关数据作为重要数据申报数据出境安全评估。这一规定减轻了企业企业对于识别重要数据的合规压力。而从个人信息的监管角度考察，医药企业需要判断其出境的数据涉及的个人信息的数量是否达到《跨境流动规定》项下的不同阈值，以及其是否涉及敏感个人信息。

如前所述，《个人信息保护法》将敏感个人信息定义为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。GB/T 35273-2020《信息安全技

术 个人信息安全规范》在附录 B 列举了敏感个人信息类型，其中就包括(i)个人生物识别信息，如个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等，以及(ii) 个人健康生理信息，如个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等。

当然，判断的前提是，相关数据构成个人信息，即《个人信息保护法》所规定的“个人信息是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，不包括匿名化处理后的信息”。在临床试验等场景中，受试者等个人的身份一般已通过受试者鉴认代码等方式进行了去标识化的处理（通过对应揭盲措施，其个人身份仍可以对应还原）。但该等信息是否仍然在去标识化处理后仍构成敏感个人信息呢？如前文所述，从目前一些省级网信办等监管部门咨询的态度来看，取决于其是否可以改变“敏感”的性质。如果经过去标识化处理的敏感个人信息被泄露或者非法使用，且泄露和非法使用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，那么经过去标识化处理的“敏感个人信息”不再属于敏感个人信息。由于目前官方尚未对医药领域的该定义有更为明确的解释，考虑到医药企业的特点，从审慎的角度考虑，一些企业还是选择从严解释，以敏感个人信息的角度对待去标识化后的临床试验数据。

除上述角度外，在行业单行法规规定中也需要厘清相关出境数据的性质。最为典型的是《人类遗传资源管理条例》(“《人遗条例》”) 等法规规定的人类遗传资源信息。根据《人遗条例》的规定，人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料，而人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。《人类遗传资源管理条例实施细则》(“《人遗细则》”) 进一步指出，人类遗传资源信息包括利用人类遗传资源材料产生的人类基因、基因组数据等信息资料，不包括临床数据、影像数据、蛋白质数据和代谢数据。相关数据的出境也涉及对于人类遗传资源的特殊监管。在临床试验等场景中，此类信息是较长涉及的。

四十八、 医药行业数据跨境传输的主要合规义务有哪些？

如前所述，从网信部门的监管角度来看，医药企业需要根据自身及相关数据的具体属性，结合数量等其他信息判断医药企业需要履行何种合规路径（申报并通过数据出境安全评估、订立并备案个人信息出境标准合同或通过个人信息保护认证）。

如前述，在判断其是否构成 CIIO 的基础上（目前实操中大多数企业并未被认定为 CIIO），医药企业需要进一步从数量及数据性质等角度考察，并据此判断其履行的合规路径（具体内容请参照《上篇：基础篇》“四、现行数据出境制度下的三条合规路径是什么？如何判断？”部分））。鉴于《跨境流动规定》第二条的规定，医药企业在“重要数据”角度已经得到了较大程度的“松绑”。而在处理个人信息数量和敏感个人信息的“门槛”上，医药企业仍需要基于《跨境流动规定》作出判断，进而选择合适的合规路径。一些研发能力较强的企业结合其临床试验等场景的情况，可能需要综合判断其是否达到数据出境安全评估的门槛。而对于一部分规模有限，尚未全面“铺开”管线的医药企业而言，其可能需要选择订立并备案个人信息出境标准合同。

除此以外，基于《个人信息保护法》等法规的有关规定，境内医药企业还需要完善其他的合规措施，如(i)根据《个人信息保护法》的规定向受试者等有关个人告知跨境传输的有关事项，并取得个人的单独同意（据此更新其知情同意书等文件）；(ii)进一步加强数据流转和处理的分类分级管理工作，包括将企业内部数据与外部供应商的数据的分别管理，将普通数据与敏感个人信息予以分类管理等；(iii)进一步加强对境外接收方的数据合规监督和管理，比如建立集团内统一的个人信息和数据管理制度，采取广泛的去标识化和加密等技术措施，要求境外接收方与相关再传输方（第三方）签署协议，确保其个人信息处理活动达到中国相关法律法规规定的个人信息保护标准等。

从人类遗传资源的监管角度，医药企业向境外传输人类遗传资源信息时也需履行有关法定义务。

根据《人遗条例》等法规的要求，外国组织及外国组织、个人设立或者实

际控制的机构（即其规定的外方单位）需要利用我国人类遗传资源开展科学研究活动（包括临床试验）的，应当采取与中方单位合作的方式进行，并需要报中国人类遗传资源管理办公室（“人遗办”，自2024年5月1日起其由科学技术部下设调整为由国家卫健委负责）审批/备案。在外方单位的参与过程中，不论是由外国组织直接参与，还是由其设立/控制的境内机构参与，都可能涉及直接或间接与境外主体分享人类遗传资源。

在开展国际合作临床试验的过程中，存在国际合作科学研究审批以及国际合作临床试验备案的两种途径。

具体而言，采取国际合作临床试验备案途径时，一般需要满足以下条件：

(1)系为获得相关药品和医疗器械在我国上市许可而开展的临床试验（一般包括Ⅰ、Ⅱ、Ⅲ期临床试验与生物等效性试验（BE）；

(2)不涉及人类遗传资源材料出境。

(3)在临床机构内利用我国人类遗传资源开展（(a)涉及的人类遗传资源采集、检测、分析和剩余人类遗传资源材料处理等在临床医疗卫生机构内进行，(b) 涉及的人类遗传资源在临床医疗卫生机构内采集，并由相关药品和医疗器械上市许可临床试验方案指定的境内单位进行检测、分析和剩余样本处理）；

在满足前述条件的情况下，国际合作临床试验不需要获得审批，仅需要事前向人遗办备案。如不能满足前述三个条件，则应选择国际合作科学研究审批的路径。此外，合作双方还应当在国际合作临床试验结束后6个月内共同向人遗办提交合作研究情况报告。

除此以外，将人类遗传资源信息向前述外方单位提供或者开放使用的，中方信息所有者还应当向科技部事先报告并提交信息备份。已取得前述许可/备案的临床试验过程中，如国际合作协议中已约定产生的人类遗传资源信息由合作双方使用，则不需要单独再事先报告和提交信息备份。另外，该种情况下，可能影响我国公众健康、国家安全和社会公共利益的，应当通过国务院科学技术行政部门组织的安全审查。

除上述规定以外，亦存在健康医疗大数据等角度的单行法规和规范、规则，

医药企业在数据跨境传输的过程中也应予以关注。

四十九、 通过境内数据交易所进行跨境数据贸易应考虑哪些跨境数据合规问题？

根据中国信通院数据显示，2023 年我国数字经济规模可达 56.1 万亿元，数字经济占 GDP 比重接近于第二产业，占国民经济的比重，达到 40%以上。伴随数字技术兴起以及各项数字经济相关的政策和法律的落地，以跨境数据流动为底层支撑的跨境数字贸易迎来蓬勃发，深刻改变了传统国 际贸易体系。[32]

跨境数据贸易的渠道主要分为以数据交易所作为跨境贸易平台的场内交易以及在数据贸易买卖双方之间以点对点方式开展的场外跨境数据贸易。目前我国数据交易市场仍处于起步阶段，我国场外数据交易体量在总体数据交易体量的占比约为 95%，场内交易规模极很小。[33]而场外更多是点对点的直接交易，并且依赖于交易合同的订立，数据的流通次数还不够高。

就场内交易，在我国相关政策法律支持与保障的背景下，数据交易所在数据跨境贸易中的作用逐渐显现。就主流的交易所而言，2022 年北京国际大数据交易所研发的北京数据托管服务平台正式投入使用，成为我国首个可支持企业数据跨境流通的数据托管服务平台。以标准统一化、管理高效化、服务定制化为特点，支持提供数据托管、脱敏输出、融合计算、建档备案等服务。目前，数据托管服务平台已落地试点。上海数据交易所积极拓展国际数据流通交易市场，建立与海外平台数据双向流动合作机制，成立国际专区板块，并与海外平台建立了数据双向流动的合作机制，创新了“数据交易所+全球性数字平台”的商业模式。深圳数据交易所在跨境数据交易等方面取得一系列创新的示范性成果，积极探索数据跨境试点。毗邻香港、澳门，深数所牢牢把握自身位于粤港澳大湾区的独特地缘优势，成功落地国内首单场内跨境数据交易。

场内的跨境数据贸易涉及数据跨境流通，因此也涉及数据出境的合规问题。

[32] 参考中国信通院《年中国数字经济发展研究报告》(2023 年)。
[33] 钛媒体：《我国数字经济正在迈向新阶段》。

对于通过场内交易的额数据产品，由于国内目前的法律并没有特别规定任何出境合规的豁免机制，因此在法律层面上，通过数据交易所进行数据出境贸易，也仍然要按照现有的数据出境的法律规定履行相应的数据出境和数据合规措施。此外，作为交易平台的数据交易所也会对拟进行数据出境贸易的产品进行独立的数据合规与安全审查，以及要求数据提供方提供第三方专业机构（例如律所）出具的合规审查报告。

例如根据我们对公开信息的调研，深数所完成的国内首单场内出境跨境数据交易，标的是数库（上海）科技公司研制“数库 SmarTag 新闻分析数据”产品。数据产品提供方向深数所提供信息收集表单，收集交易标的、交易双方、交易场景、数据安全等交易基础信息，对于国家的和地方相关部门要求申报和审批（例如数据安全审查和出境评估）的要提供相应材料，作为交易的“自证”材料；此外，数据产品提供方还委托专业律所机构出具对该笔交易合规评估的法律意见书，对数据交易中的合规风险进行披露，该材料将作为“他证”材料，同“自证”材料一起提供至深数交。交易方自证及他证合规材料的基础上，深数所对数据出境、处理、流通、管理、技术措施、合法性、安全性等进行了大量的合规评估工作。最终撮合成交总金额约 500 万元的 5 笔交易。

五十、 公共数据运营主体是否可以就公共数据对境外主体进行授权使用或开放共享？

《数据二十条》将数据分为公共数据、企业数据、个人数据[34]。根据《数据二十条》以及各地政府的数据条例和公共数据运营相关的行政法规和规章，公共数据是指对各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。在公共数据运营这样的背景下讨论本问题，涉及的另一层的问题则是，因各地公共数据的运营均应按照“原始数据不出域、数据可用不可见”的要求运营公共数据，因此在公共数据运营方谈及的公共数据，一般已经不是原

[34] 《关于构建数据基础制度更好发挥数据要素作用的意见》（三）探索数据产权结构性分置制度。建立公共数据、企业数据、个人数据的分类分级确权授权制度。中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见_中央有关文件_中国政府网 (www.gov.cn)。

始数据或仅经过初步治理的公共数据资源，而是在公共数据授权使用或有条件共享开放的环节中涉及的公共数据产品。[35]

根据各地省市的数据条例或者公共数据运营相关的行政法规和规章，公共数据可在合法合规安全的前提下，对外进行授权使用或者开放共享。特别是，很多省市地方政府将公共数据基于分级分类授权的规则，规定了有条件授权使用和开放和共享的机制。然而，数据二十条也规定了，在鼓励公共数据在保护个人隐私和确保公共安全的前提下，公共数据运营主体应按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供。那么在这样的基础制度下，对于位于境外的主体（特别需要境内公共数据运用训练模型的境外企业），是否也可以成为公共数据授权使用或开放共享的对象呢？

这是一个比较复杂的问题并且也需要根据公共数据授权运营主体的具体的运营模式而进行具体个案分析。对于上述问题，目前现有法律法规并没有禁止性的规定，因此在符合法律合规和安全等要求的前提下，境外的主体通过可行的技术方式也可以获得境内的公共数据。

从法律角度来说，就公共数据的对外授权使用或共享开放领域，境外主体应注意和考虑以下几个重点的数据合规问题：

首先，根据《促进和规范数据跨境流动规定》（以下简称“《规定》”），境外主体获得境内的公共数据属于数据出境范畴。因此，对于这类公共数据的出境情形，应结合具体的场景和产品按照《规定》履行相应的数据出境合规义务。

其次，对于拟出境的公共数据，建议还要进行数据安全的审查，即应判断出境的公共数据是否含有核心数据、国家秘密、重要数据、涉及国家安全等敏感信息。如果存在，则不得出境或者需完成数据安全审查和整改后再出境。此外，根据数据安全法的相应规定，即使境外主体能够合法合规地获得公共数据，也可能触发数据本地存储、出口管制等其他法律合规要求和限制性要求。对于上述的合规问题的具体细节，可参考本合规实务的相应部分，在此不做赘述。

再次，如果公共数据中含有个人信息，那么相应的个人信息因数据出境本

[35] 这里的数据产品的概念，是广义的概念范围，即这里提及的“数据产品”包括但不限于统计数据、数据集、数据服务、数据应用、数据产品，例如以模型、核验等产品和服务等形式向社会提供的数据产品。

身超出了原始公共数据采集和获取时的目的和范围，因此数据提供方还应注重履行个人信息保护法的相应合规要求，例如对个人进行告知和获得对出境的单独同意等。具体可以参考本合规实务相应的问题答复内容。当然，我们也可以预见，这样的告知和获取同意需要有效的渠道，往往在公共数据领域比较难以获得。此外，公共数据运营企业与境外主体还应签署对数据提供方和数据本身有充分保护度的数据授权或开放共享协议（如果在出境渠道方式上，数据提供方应适用标准合同出境，那么应按照标准合同的要求签署协议）。例如，协议中可明确约定未经提供方同意，境外主体不得随意转让、共享、授权数据给第三方使用的条款，以保护公共数据的安全使用。

另外，由于在公共数据授权使用或公开共享领域，公共数据运营主体应严格按照“原始数据不出域、数据可用不可见”的要求进行数据运营，因此境外主体也有可能涉及需通过采用隐私计算、沙箱等技术方式，在公共数据运营的平台上去获得其需要的数据或数据结果。为此，境外主体可能需要向公共数据运营方提供其数据模型，因此也可能涉及境外主体在其管辖权领域数据跨境的合规问题，以及在数据模型与“可用不可见”的数据进行碰撞之后，以及再以合法安全的方式获取碰撞后的数据的合规出境问题。

因公共数据的出境既涉及公共数据领域的数据合规问题，也涉及数据出境的合规问题，因此我们也建议公共数据运营主体和境外主体在遇到类似问题时尽早全面咨询专业的法律顾问。

附件一、国家及各地省级网信部门联系方式

单位	办公地址	联系电话
国家互联网信息办公室	北京市西城区车公庄大街 11 号	数据出境安全评估申报：010-55627135
		个人信息出境标准合同备案：010-55627565
		个人信息保护认证申请：010-82261100
北京市互联网信息办公室	北京市朝阳区华威南路弘善家园 413 号	010-67676912
天津市互联网信息办公室	天津市河西区梅江道 20 号	022-88355322
河北省互联网信息办公室	河北省石家庄市桥西区维明南大街 79 号	0311-87909716
河南省互联网信息办公室	河南省郑州市金水区金水路 16 号	0371-65901067
浙江省互联网信息办公室	浙江省杭州市西湖区省府路 29 号	0571-81051250
上海市互联网信息办公室	上海市徐汇区宛平路 315 号	021-64743030-2711
江苏省互联网信息办公室	江苏省南京市建邺区白龙江东街 8 号	025-63090194
福建省互联网信息办公室	福建省福州市鼓楼区北大路 133 号	0591-86300613
安徽省互联网信息办公室	安徽省合肥市包河区中山路 1 号	0551-62606014
重庆市互联网信息办公室	重庆市渝北区青竹东路 6 号	023-63151805

单位	办公地址	联系电话
贵州省互联网信息办公室	贵州省贵阳市云岩区宝山北路 39 号	0851-82995001/82995061
山东省互联网信息办公室	山东省济南市市中区经十路 20637 号	0531-51773249/51771297
广东省互联网信息办公室	广东省广州市越秀区中山一路 104 号	020-87100794/87100793
陕西省互联网信息办公室	陕西省西安市雁塔区雁塔路南段 10 号	029-63907136
甘肃省互联网信息办公室	甘肃省兰州市城关区南昌路 1648 号	0931-8928721
山西省互联网信息办公室	山西省太原市迎泽区五一路 36 号	0351-5236020
江西省互联网信息办公室	江西省南昌市红谷滩区卧龙路 999 号	0791-88912737
云南省互联网信息办公室	云南省昆明市西山区日新中路 516 号	0871-63902424
湖北省互联网信息办公室	湖北省武汉市武昌区水果湖路 268 号	027-87231397
湖南省互联网信息办公室	湖南省长沙市芙蓉区韶山北路 1 号	0731-81121089
青海省互联网信息办公室	青海省西宁市海湖新区文景街 32 号	0971-8485510
辽宁省互联网信息办公室	辽宁省沈阳市和平区光荣街 26 号甲	024-81680082
吉林省互联网信息办公室	吉林省长春市朝阳区新发路 666 号	0431-82761087
黑龙江省互联网信息办公室	黑龙江省哈尔滨市南岗区华山路 12 号	0451-58685723

单位	办公地址	联系电话
海南省互联网信息办公室	海南省海口市国兴大道 69 号	0898-65380723
四川省互联网信息办公室	四川省成都市青羊区桂花巷 21 号	028-86601862
广西壮族自治区互联网信息办公室	广西壮族自治区南宁市青秀区民族大道 112 号	0771-2093017/2093049
宁夏回族自治区互联网信息办公室	宁夏回族自治区银川市金风区康平路 1 号	0951-6668938
西藏自治区互联网信息办公室	西藏自治区拉萨市城关区农科路 7 号	0891-6591509
内蒙古自治区互联网信息办公室	内蒙古自治区呼和浩特市赛罕区银河南街 8 号	0471-4821277
新疆维吾尔自治区互联网信息办公室	新疆维吾尔自治区乌鲁木齐市新市区西环北路 2221 号	0991-2384855
新疆生产建设兵团互联网信息办公室	新疆维吾尔自治区乌鲁木齐市天山区中山路 462 号	0991-2899091

《实务问答》出品

威科先行

联合发布单位及作者

环球律师事务所

孟洁 李玲 刘展 张桐 董杰睿

对外经济贸易大学数字经济与法律创新研究中心

许可

蔚来控股有限公司

高岗 王诗笋 谌棋

奇安信科技集团有限公司

马兰 刘前伟 刘洪亮

北京奥美互动咨询有限公司

殷振华

杭州有赞科技有限公司

方子雯 陈昕 魏东杰

其他作者

郭俊彤 田亮 王程 尹童晖

免责声明：

本文件不代表所有联合发布单位对有关问题的法律意见，任何仅依照本文件的全部或部分内容而做出的作为和不作为决定及因此造成的后果由行为人自行负责。如您需要提供法律意见或其他专业意见，应该向具有相关资格的专业人士寻求专业的帮助。

联系方式：

E. mengjie@glo.com.cn