路转溪头：个人信息出境三条路径的选择和执行

作者：杨迅 | 象玉婷 | 夏雨薇

近日，有关个人信息出境的规定频繁出台，个人信息出境的三条路径也日渐清晰地展现出来。有信息出境需求的企业，尤其是跨国公司，面对严格的个人信息出境合规要求，应当如何应对呢？

目 录

一. 个人信息出境的法律体系

随着 2017 年 6 月 1 日《网络安全法》的颁布后，数据出境合规成为了被广泛关注的问题。然而最初的信息出境评估要求仅针对关键信息基础设施的运营者(**"CIIO"**)。根据《网络安全法》第三十七条，关键信息基础设施的运营者在中国境内运营中收集和产生的个人信息和重要数据应当在境内存储，因业务需要确需向境外提供的，应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。《网络安全法》并未对非关键信息基础设施运营者向境外提供个人信息或重要数据的行为提出监管要求。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

此后，国家互联网信息办公室于 2021 年依次发布的《数据出境安全评估办法(征求意见稿)》以及《网络数据安全管理条例(征求意见稿)》中，进一步扩大了数据出境需要进行安全评估的范围，例如将出境数据中包含重要数据或者处理个人信息达到一百万人的个人信息处理者纳入了安全评估的范围，但上述征求意见稿缺乏上位法的支撑，且颇具争议，因此一直未落地实施。

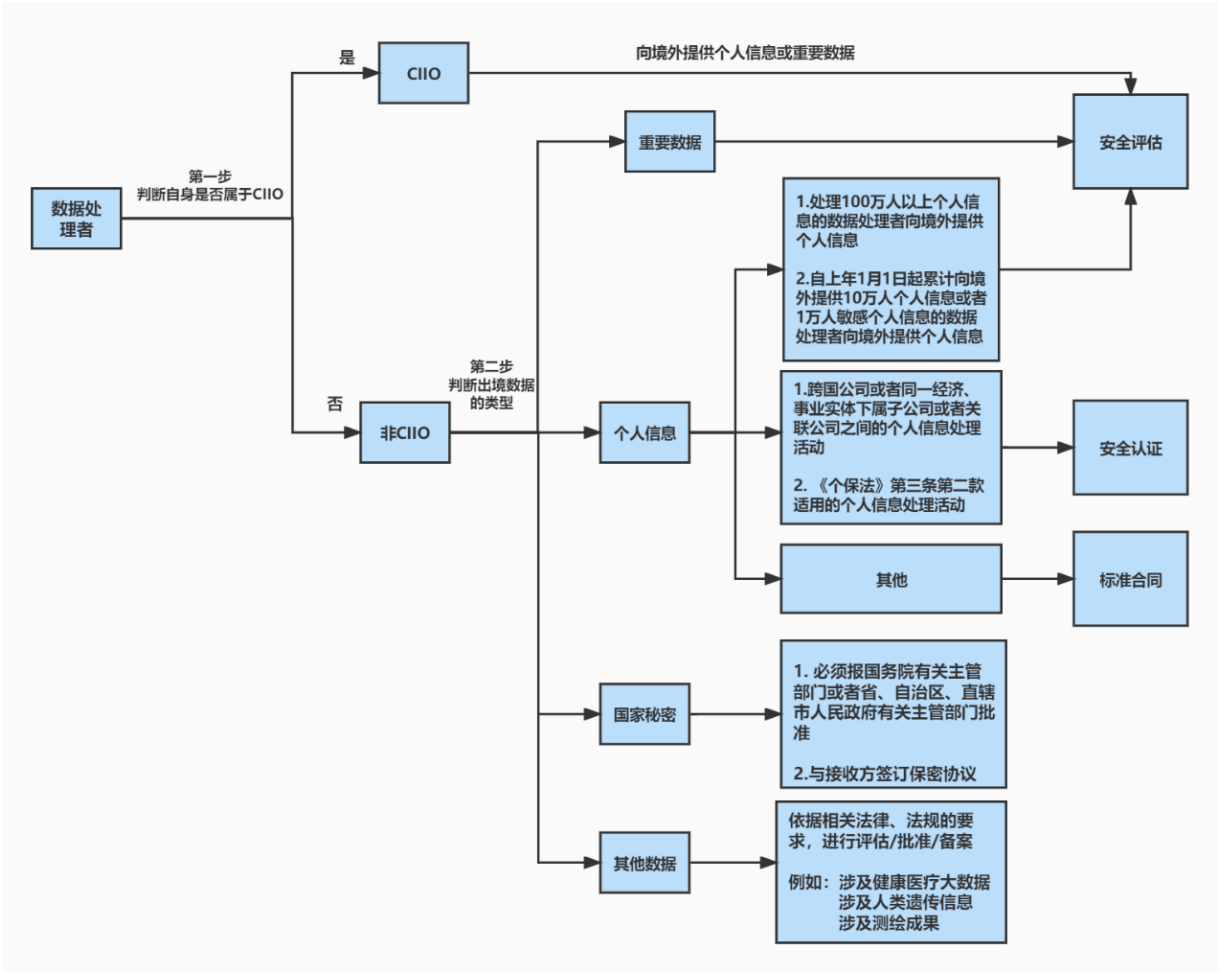
2021 年出台的《数据安全法》和《个人信息保护法》分别提出了 CIIO 和非 CIIO 出境重要数据和个人信息的监管要求。其中，2021 年 6 月 10 日国家出台的《数据安全法》采取了"分层监管"的方式，要求 CIIO 在境内运营中收集产生的重要数据必须进行安全评估，并且，其他数据处理者出境重要数据时，应当按照国家网信部门制定的数据出境安全管理办法来进行。2021 年 8 月《个人信息保护法》("**《个保法》**")正式公布，其中第三十八条规定了个人信息处理者因业务需要，向境外提供个人信息的需要具备以下条件之一: (1)通过出境安全评估; (2)进行个人信息保护认证; (3)与境外接收方订立标准合同。其中第五十五条，进一步将个人信息出境规定为必须事前进行个人信息保护影响评估的情形之一。

《个保法》虽然提出了信息出境的三条路径: 安全评估、保护认证和标准合同。但在《个保法》出台的时候，国家网信部门尚未制定安全评估的办法，如何开展个人信息保护认证亦未明确，标准合同也没有颁布，所以业界对于个人信息如何出境仍处于迷茫的状态。实践中，我们通常会建议相关企业或机构按照《信息安全技术 数据出境安全评估指南(征求意见稿)》以及《信息安全技术 个人信息安全规范》("《个人信息安全规范》")等国标的要求，以尽可能接近预测中的标准合同的方式与境外的接收方签订相关法律文件，并自行开展个人信息保护影响评估，以满足个人信息出境的法律合规要求。

但是，近日个人信息出境的三条路径已见端倪。2022 年 6 月 24 日，全国信息安全标准技术委员会发布了《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》(**"《认证规范》"**)，为认证机构实施个人信息跨境处理活动提供了认证依据。6 月 30 日，国家互联网信息办公室()发布《个人信息出境标准合同规定(征求意见稿)》(**"《标准合同规定》"**)，并在附件中公布了个人信息处理者和境外数据接收方签订的标准合同范式。2022 年 7 月 7 日，国家互联网信息办公室进一步发布了《数据出境安全评估办法》(**"《评估办法》"**)，明确了数据处理者向境外提供数据时适用国家网信部门评估的情形、内容、流程等。至此，《个保法》第三十八条项下的三种个人信息出境方式的框架基本成型。对于有个人信息出境需求的相关企业和机构而言，应当结合自身的业务情况以及法律合规要求，选择合适的个人信息出境方式。

二. 个人信息出境的路径选择

对于企业或相关机构而言，在数据出境前需要根据企业自身的属性，以及拟出境的数据种类、数量，来综合判断需要承担何种合规的义务，以及如何选择合适的数据出境路径。



注：《个保法》第三条第二款的情形包括(i)以向境内自然人提供产品或者服务为目的; (ii)分析、评估境内自然人的行为; (iii)法律、行政法规规定的其他情形。

对于出境重要数据的，根据《评估办法》的规定，数据处理者向境外提供重要数据必须进行数据出境安全评估；对于个人信息的出境，相关企业或机构可以按照《评估办法》和《认证规范》来决定个人信息出境的路径，即:

(1) 通过国家网信部门组织的**安全评估**(参见《数据出境安全评估办法》);

(2) 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**(参见《网络安全标准 个人信息跨境处理活动认证技术规范》);

(3) 按照国家网信部门制定的标准合同与境外接收方**订立合同**(参见《个人信息出境标准合同规定(征求意见稿)》)。

具体而言，向境外提供个人信息落入以下范围的，需要安全评估:

(1) **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。**此处的“处理”包括收集、使用、储存等个人信息的处理行为。举例而言，如果某企业储存了 100 万条以上的个人信息，那么企业之后出境任何数量的个人信息，均需要进行数据出境安全评估。由此，我们建议企业应当对自身储存的存量个人信息进行管理，及时将不必要的或超出了储存时限的个人信息进行删除或匿名化处理，一方面可以降低行政管理负担，另一方面可以减轻企业数据出境的合规成本。

(2) **关键信息基础设施运营者向境外提供个人信息。**现阶段识别 CIIO 的参考依据主要包括《网络安全法》、《关键信息基础设施安全保护条例》、《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)》等,CIIO 的认定工作由各行业的主管部门进行认定和通知。若企业被认定为 CIIO,则只要其向境外提供个人信息,就需要进行数据出境安全评估。

(3) **自上年 1 月 1 日起累计向境外提供 10 万人个人信息或 1 万人敏感个人信息的数据处理者向境外提供个人信息**。此处 10 万人个人信息或 1 万人敏感个人信息指的是“人数”而非“人次”,无论个人出境的个人信息数量多少,均按照 1 人来计算。由此可见,数据出境安全评估关注的更多的是影响面,即对社会公共利益以及涉及的人数的考量,而非对具体的个人权益的影响(如涉及的具体个人信息是否全面、完整以及是否能形成个人信息用户画像等),这也是我国个人信息立法理念与欧洲相关立法理念上的区别。

对于下列个人信息出境的行为,可以适用个人信息保护认证:

(1) **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**。本项通常适用于跨国公司内部的信息流动,在这种流动中,跨国公司的内部管理体系和 IT 设置将被纳入认证的考察范围。

(2) **《中华人民共和国个人信息保护法》第三条第二款适用的个人信息处理活动。**即,在境外为分析境内自然人行为或者为向境内自然人提供商品或货物而处理境内自然人信息的。类似地,在此种情况下,个人信息认证亦将考察境外信息处理者的信息管理能力和技术水平。

三. 三条路径下个人信息出境的必备条件

结合《认证规范》、《标准合同规定》以及《评估办法》的相关规定,对于个人信息处理者而言,无论其选择哪一种出境路径,除了取得个人的单独同意外,其均需要满足以下两项必备条件:

其一,**与境外的数据接收方签订法律文件。**与境外接收方签订符合规范的法律文件,既是《个人信息安全规范》下的要求,也是《个保法》下涉及委托境外第三方处理个人信息时的法定义务,个人信息处理者必须与受托人约定处理的目的、期限、处理方式、种类、保护措施以及双方的权利义务等内容。在签署相关法律文件时,个人信息处理者不仅应当满足上述法律或国标的要求,还应当参照《标准合同规定》进行比对,不能违背《标准合同规定》的相关规定。若企业选择了签订标准合同作为个人信息的出境路径,则必然需要满足《标准合同规定》的相关规定;若企业选择了进行出境安全评估,或个人信息保护安全认证作为出境的路径,与境外接收方签订法律文件仍是一个重要的考量因素。虽然《评估办法》和《认证规范》均未要求企业必须签订标准合同,但标准合同反映了政府对数据跨境处理的相关法律文件应当达到的安全保护水平的期望。因此,若无特殊情况,企业应当保证签署的相关个人信息出境法律文件,能够满足标准合同的基本要求。

其二,**开展个人信息出境风险的自评估。**根据《评估办法》第五条的规定,数据处理者在申报数据出境安全评估前,应当开展数据自评估;根据《认证规范》第 4.4 条的规定,开展个人信息跨境活动的个人信息处理者应当事前进行个人信息保护影响评估;根据《标准合同规定》第五条的规定,个人信

息处理者向境外提供个人信息前，应当事前开展个人信息保护影响评估。因此，无论选择哪一种个人信息出境路径，企业均需要开展数据出境风险自评估。

对于企业开展的个人信息出境风险自评估，具体需要达到何种安全保护标准，企业的出境行为才能被允许，相关法律法规并未明确规定。企业需要结合自身的业务情况，按照一定的流程和预先设定的评估框架，对某个特定的个人信息出境场景进行风险判定，并决定是否应当进一步采取安全保护措施以降低风险。若企业选择了签订标准合同作为个人信息出境的方式，则此时将由企业自行开展出境风险评估，与之相关法律责任将由企业自身承担；若企业选择了安全评估或个人信息保护认证作为出境的路径，则风险自评估将作为一个基础，后续将由国家网信部门进行安全评估或由专业机构进行认证。

四. 个人信息出境带来的挑战

随着个人信息出境制度日见雏形，摆在个人信息出境企业面前的，可能是更加严格的出境监管要求。这就需要企业投入更多的合规成本。

1. 成本增加

个人信息跨境处理的合规要求提高了个人信息出境方的数据治理成本。如上文所述，个人信息出境虽然存在三条路径，但都有相类似的前置条件。无论是 6 月生效的《认证规范》、9 月生效的《评估办法》，还是征求意见中的《标准合同规定》，都规定了个人信息出境方应当进行个人信息出境安全评估，亦应当与境外接收方签订合同(或直接签定标准合同)以规范个人信息出境各方的责任与义务。

首先，个人信息出境安全评估的要求意味着个人信息出境方应当建立动态的评估制度。鉴于不同的个人信息出境活动涉及不同的出境“目的”、“范围”和“种类”，其合法性、正当性以及必要性与数据的敏感程度也因此有待个案评估。也就是说，个人信息出境方难以通过“流水线”式的机械化流程，对个人信息出境活动进行一揽子的风险评估。个人信息出境方需要建立动态的评估体系。

此外，在进行评估时，个人信息出境安全评估需要引入不同领域的专业人员。评估不但包含合法性、正当性以及必要性这些法律元素，还需要考虑个人信息出境活动的业务场景，采取的安全技术措施、应急处理措施与个人信息主体的行权途径与方式等技术和管理因素。这也说明个人信息出境活动不但需要专业的法律意见，还需要 IT、合规、业务等多个部门合作，提供专业建议与改善措施。值得一提的是，《认证规范》更进一步明确要求，当个人信息出境方通过相关专业机构的认证进行数据跨境传输时，应当任命专业的个人信息保护负责人以及设立专业的个人信息保护机构统筹规划与上述个人信息出境安全评估相关的工作。

进一步地，个人信息出境安全评估需要视情况不断更新。针对达到一定数量而需要通过省级网信部门提交国家网信部门进行审批的出境安全评估，即使相应的评估报告报批通过的，有效期

也只有 2 年。也就是说，无论是有效期届满，或是有效期内个人信息出境情况发生变化可能影响数据出境安全的，个人信息出境方皆需根据实际情况重新评估并重新申报。

最后，即使个人信息出境方不选择通过签订标准合同的方式跨境处理个人信息，个人信息出境方仍需要根据相关法律法规的要求签署规范跨境传输活动各方权利与义务的相关协议(简称"**法律文件**")。

有个人信息出境需求的企业应当注意，在个人信息出境相关法律法规正式实施且其给予的过渡期届满后，签订符合法律法规要求的法律文件(或直接签署标准合同)，并对相关的跨境数据传输行为进行评估，将会成为所有公司数据治理活动中的必然常态。公司需要对内部的人员、资源与流程进行调配、升级与长远规划，这将不可避免产生相应的内控成本。

2. 管理境外数据接收方

订立个人信息出境相关合同时主要由信息接收方对其基本信息、资质能力以及承担的数据安全责任作出承诺。而开展出境安全评估时，个人信息出境方需自身尽注意义务调查与核验合作方的基本信息、相关资质能力。

结合各路径下的法律法规，目前个人信息出境方可能需要了解并确认:

1) 接收方的基本信息;
2) 接收方所在国家或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;
3) 接收方的数据保护水平、管理和技术措施与能力;
4) 数据安全和个人信息权益是否能够得到充分有效保障，以及保障方式。

结合 2017 年的《信息安全技术 数据出境安全评估指南(征求意见稿)》对数据出境安全评估的相关意见，对接收方数据保护水平的评估不但包含其管理制度保障能力以及技术措施保障能力，还需要考虑其数据处理历史，是否出现过任何数据安全事件且该事件是否得到有效处置等。这也说明，个人信息出境方不得依赖于境外接收方在相关的合同中做出的承诺，还需要提前对境外接收方进行背景调查，自行确认合作时的风险等级。

3. 法律适用问题

目前，《评估办法》《认证规范》中均要求个人信息出境双方订立约定了数据安全保护责任义务的法律文件并列明必备条款。虽然《标准合同规定》仍在征求意见的阶段，但其附件的标准合同对意图通过签署标准合同出境数据的个人信息出境方而言也具有极高的参考价值。其中，就法律文件(或标准合同)的法律适用问题，从商务角度考虑，对个人信息出境方仍有较高难度。

《标准合同规定》要求标准合同准据法为中国大陆法律，同时要求境外接收方必须根据**中国法律法规**对外提供个人信息，并履行报告个人信息安全事件、响应个人信息主体等义务，标准合同

下“中国法律法规”的定义较广，极有可能涉及到了合同延及的所有中国法律法规。如《标准合同规定》最终生效，境外接收方处理数据的活动，在很大程度上将受制于中国法律法规。此外，标准合同还赋予了个人信息主体“第三方受益人”的法律地位，个人信息主体有权基于合同基础要求标准合同下的境外接收方履行相应的个人信息保护义务。

而《认证规范》也要求境外接收方应当承诺“接收认证机构监督”、并接受“中国个人信息保护相关法律、行政法规管辖”、“确保不低于中国个人信息保护相关法律、行政法规规定的标准的个人信息保护水平”。此外，《认证规范》也强调了个人信息主体也是相应法律文件与个人信息主体权益相关条款的**受益人**。

《评估办法》虽也要求出境双方签署相应的法律文件，但并没有对具体的条款作出详细的规定。不过，考虑到相应的评估报告并不只是留档备查而是需要直接交由国家网信部门进行审批，对该类法律文件的审阅标准想必也趋于严格。

从商业安排角度考虑，让出境接收方承诺，相应的合同受到中国法律的管辖，且可能需要遵守众多不明确的中国法律法规(甚至可能超出个人信息保护相关的法律法规范围)，认可个人信息出境方与个人信息主体的双重监督，难度较大。合同是个人信息出境活动的必要前提，这也给个人信息出境方推进合同订立、进行个人信息出境安全评估等环节带来了不小的难度。

五. 实务建议

目前，我国关于个人信息出境的监管流程和体系基本建立完成。个人信息出境方也亟需在新法生效前做好准备。

短期内，个人信息出境方应当意识到，签署规范出境双方权利与义务的合同条款，在内部进行个人信息出境安全评估，都将成为个人信息出境方进行数据治理的必要事务与常态。这也就要求个人信息出境方对内部流程进行设计与整合。将个人信息出境安全评估纳入到企业的管理流程中去，不但需要明确如何发起、进行、完成个人信息出境安全评估，还需要明确如何统筹多部门分工合作，如何指派主要的负责人以及如何设立负责机构等若干事宜。

特别是对于需要向网信部门申报个人信息出境安全评估的企业而言，《评估办法》仅给予个人信息出境方自该法生效后 6 个月的过渡期，要求个人信息出境方在过渡期内整改内部已经开展的不合规的个人信息出境活动。

我们建议，如想要尽快建立健全内部个人信息出境评估流程，个人信息出境方应立即开展个人信息出境安全评估内部流程的构建，对已经开展的个人信息出境活动根据企业自身的属性以及出境数据的类型进行路径归类。并进一步在相同的个人信息出境路径下建立红白名单制度，即个人信息出境活动的具体目的较为相似、个人信息出境接收方的主体可信程度较高、数据处理目的较为简单、风

险较小的个人信息出境活动，可以统一归类于**“白名单”**，反之则落入**“红名单”**。在评估新的个人信息出境活动时，企业可参考历史上的“红白名单”借鉴必要措施和方案。

长远来看，实现数据本地化部署也是值得个人信息出境方考虑的一种解决方案。毕竟，除不得不长期对个人信息出境活动进行监管外，个人信息出境方还可能面对更多的考验与不确定性。譬如我们在本文提到的关于受到监管的“**处理 100 万人以上个人信息的数据处理者**”之定义，如立法者此处意图规制该等数据处理者的任一数据出境活动的，数据处理者只得更加谨慎地处置每一次数据出境行为。

搭设相应的信息系统将高敏感的数据存储在中国境内进行数据本地化部署，将降低个人信息出境活动的频率，进而缓解数据跨境传输所带来的技术与法律层面的风险。同时，数据本地化部署后，个人信息出境方不再需要对大量的个人信息出境活动进行动态监管，这也将进一步优化个人信息出境方的数据治理体系与成本预算。

如您希望就相关问题进一步交流，请联系:

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

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

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野