个人信息出境规则新动向

作者：潘永建 | 杨迅 | 杨坚琪 | 胡鑫超

数字经济方兴未艾，正在日益与互联网、人工智能、云计算等行业深度融合发展。数据是数字经济的重要支撑，已成为除土地、劳动力、资本和技术外的第五类“生产要素”。数据保护与规范亟需法律从个人信息与隐私保护、企业数据权益、国家安全与监管等维度作出系统性的制度安排。作为数据保护制度的基础法律，《个人信息保护法》和《数据安全法》的重要性毋庸置疑。2021 年 4 月 29 日，《个人信息保护法(草案二次审议稿)》《数据安全法(草案二次审议稿)》公布。从企业使用数据和合规遵从的视角，通力网安数据业务小组对审议稿作出系列解读，本文为第一篇《个人信息出境规则新动向》。

作为《个人信息保护法》中最受到业界关注的制度之一，“个人信息出境要求”是国际机构和在华跨国企业长期重点关注的内容。无论是政府间协同执法、跨境业务活动，还是大型企业的内部管理，国家、企业以及各类组织在数字化时代都不可避免地会存在个人信息的跨境传输需求。《个人信息保护法(草案二次审议稿)》(以下简称“**《二审稿》**”)基本维持了《个人信息保护法(草案)》(以下简称“**《一审稿》**”)建立的“以自我评估为主，特定类型的出境需要政府评估”的个人信息出境制度，但在细节上略微作出了调整。本文将简要梳理个人信息出境制度的相关规定，总结《二审稿》中的重点内容，以期通过分析相关立法趋势和监管要点，为企业的个人信息出境活动提供实务建议。

一. 个人信息出境规定的“前世今生”

全球化和数字化时代，网络链接开始消解地缘政治意义上的物理边界，突破国界的数据跨境流动也日益频繁。在“棱镜计划”被曝光后，欧盟等政治实体在加强维护个人信息主体权利的基础上，对跨境传输实施进一步的法律限制。我国政府基于公共安全的理由，亦对跨境数据流通持保守态度：例如，2016 年颁布的《网络安全法》(以下简称“**《网安法》**”)第 37 条要求关键信息基础设施运营者(“**CIIO**”)应当将其在

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

中国境内收集的个人信息储存在中国境内，仅在业务确实需要的情况下，按照主管部门要求进行评估后方可出境。值得注意的是，《网安法》仅对 CIIO 提出要求，其他网络运营者则不受此限。

一年之后，国家互联网信息办公室(以下简称“**网信办**”)于 2017 年公布了《个人信息和重要数据出境安全评估办法(征求意见稿)》(以下简称“**《2017 办法》**”)，将个人信息本地存储及出境评估的义务主体从《网安法》下规定的 CIIO 扩大到了所有的“网络运营者”。《2017 办法》下对于个人信息出境采取了“分类监管”的模式：低于规定的出境数量的，网络运营者可以通过自评估的方式确认是否可以出境；但如果出境数量触发监管要求，则应当报请行业主管部门或网信监管部门组织安全评估。《2017 办法》突破了《网安法》的适用主体范围，相比较之后的立法，显然更注重数据流动的可行性。

2019 年年初，特朗普政府重新制定亚太策略，国际关系瞬时突变，中美经贸关系日趋紧张。尤其是，美国政府在 2018 发布的《澄清域外合法使用数据法》赋予了美国政府针对“美国企业”在世界各地存储数据的“长臂管辖权利”，更是直接引发了包括中国在内的一众国家对于境内数据权利控制的担忧。与时局的发展对应，网信办重新梳理了个人信息与重要数据的出境监管要求，并于 2019 年重新发布了《个人信息出境安全评估办法(征求意见稿)》(以下简称“**《2019 办法》**”)，将个人信息与重要数据的出境要求作出区分对待，该等区分模式延续至目前的《二审稿》中。《2019 办法》提出了极其严苛的出境要求：只要向境外提供个人信息的，网络运营者均需向省级网信部门报请评估。而且除安全评估外，《2019 办法》还要求网络运营者与个人信息接收方签订必要的数据出境相关合同，建立个人信息出境记录，并履行年度报告义务。

总结《网安法》、《2017 办法》和《2019 办法》下的个人信息出境要求，我们发现随着中国政府日益强调“数据安全”，主管部门也根据时局意图不断调整直至形成严格的出境条件；但在另一方面，顾虑到该种严格的审批制度对企业运营的影响和实践中的监管难度，其实施亦缺乏实践上的可操作性。回应各方的呼声，在中美关系趋缓的大背景下，2020 年 10 月的《一审稿》则重新制定了一套务实、可行、安全和便捷的出境管理规则。

二. 从“雾里看花”到“拨云见日”

《一审稿》为个人信息的出境管理专设一章(第三章)，可见个人信息出境问题在立法者视角下的重要性。最新版的《二审稿》延续了《一审稿》的管理规则，即根据处理个人信息主体的对象，实施不同类型的个人信息出境安全审查义务。也就是说，根据《二审稿》第 38 条至第 40 条的规定，CIIO 将和一般个人信息处理者适用不同的出境要求：

- CIIO：原则上应当将其在境内收集的个人信息储存在本地。确需向境外传输的，应当通过国家网信部门组织的安全评估；
- 一般的个人信息处理者：如果处理信息未达到规定数量的，通过专业机构的认证，或者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后，即可出境；如果处理信息达到国家网信部门规定数量的，则参照 CIIO 进行管理。

除了上述规定之外，在目前的《二审稿》下，个人信息处理者对外提供个人信息，还需要满足其他的条件，包括(1)履行告知义务; (2)获取单独同意; (3)事先进行风险评估。

尽管《二审稿》对比《一审稿》在个人信息跨境提供的总体监管框架上未作改动，但我们注意到在细节上仍然有几点调整:

首先，《二审稿》进一步“固定”了“与境外接收方”订立合同的内容。《二审稿》第 38 条第 3 款规定，境内的个人信息处理者，应当按照“网信部门制定的标准合同”，以保证出境过程的整体安全性。尽管目前网信办未能提供标准合同或其指南，通过梳理过往的立法逻辑，我们认为如下的条款或者内容很可能将会在标准合同中存在:

1. 出境基本情况，包括身份、联系方式、处理目的、处理方式、个人信息的种类;
2. 个人信息主体权利行使方式;
3. 处理者的责任和义务条款，包括但不限于获取知情同意、提供合同副本、转达诉求及先行赔付;
4. 接收者的责任和义务条款，包括但不限于实现个人信息主体权利、按照约定目的使用、遵守所在国家法律和及时通知;
5. 对接收者将个人信息传输给第三方的限制;
6. 个人信息主体合法权益受损时，处理者和接收者的连带责任;
7. 接收者国家法律环境发生变化导致合同难以履行时应终止合同或重新进行安全评估;
8. 合同终止不能免除个人信息主体合法权益有关条款规定的责任义务。

其次，在因国际司法协助和行政执法协助的需求，境内个人信息处理者向境外提供个人信息的场景中，《一审稿》提出了事先审批的要求。而《二审稿》通过对第 41 条的修订，进一步规定“在中国境内存储的个人信息”不得私自提交给境外司法或者执法机构。这个细小的变化反映了中国政府一再重申的“数据主权”理论，对于各地政府积极筹备的“离岸数据中心”业务存在一定的影响。

最后，《二审稿》第 42 条和第 43 条还进一步明确了对境外信息接受方的管辖以及中国政府实施反制措施的合法性。《二审稿》延续了《一审稿》的“域外适用”效力，根据第 3 条的规定，以“向境内自然人提供产品或者服务为目的处理行为”，以及“为分析、评估境内自然人的行为”的个人信息处理活动，即使该等处理活动发生在境外，同样受到《个人信息保护法》的管辖。同时，境外的个人信息处理者还需要在中国境内设置专门机构或者指定代表，按照监管部门要求按时履行信息报送程序。这意味着如果正式版的《个人信息保护法》按照《二审稿》的形式最终得以通过，那么在境外的信息接受方也将受到《个人信息保护法》的约束。更进一步，以“域外管辖”效力为基础，为了应对国际形势的变化，《个人信息保护法》第 42 条和第 43 条特赋予相关部门将损害个人信息权益或危害我国国家安全和公共利益的境外组织和个人列入“限制或者禁止个人信息提供清单”和对部分国家和地区采取**反制措施**的权力。该等条款的出台可能是为了应对部分国家针对中国企业实施的“非中立性制裁措施”的应对之策，例如印度政府自 2020 年开始的封杀抖音活动，美国政府于 2021 年 4 月提议的《保护美国人的数据免受外国监控法案(Protecting American’s Data from Foreign Surveillance Act of 2021)》。对于“出海企业”而言，该等条款如果最终得以通过，则意味着其同样需要关注投资所在国的政治和法律活动，以免中国政府实施的反制措施影响业务联系性。

三. 《二审稿》后的个人信息出境合规建议

加强“数据本地化”的监管，正在成为越来越多的主权国家的选择，而在华企业如果需要利用境外的数字化资源，则同样面临中国政府设置的数据出境的法律要求，例如:

- 外资医疗机构在临床试验中，通过境外母公司的服务器处理和分析数据，需要办理必要的人类遗传资源审批;
- 全球总部为实现反舞弊调查的目的，需要境内子公司向其提供客户或者员工的个人信息，但在此情况下因为不太可能获取客户或员工的同意，且客户或员工可能撤回同意，导致不满足个人信息出境的条件，全球总部因此无法获取该等数据。

《二审稿》对比《一审稿》的“变与不变”，则似乎暗示着中国立法者将基于目前的条款构建中国境内收集个人信息的出境规则。基于上述观点，我们特此提出如下建议，以提前帮助在华企业的跨境传输实践能够在《个人信息保护法》生效后平缓过渡:

1. 完善告知同意方式

根据我们的观察，目前多数企业将个人信息跨境传输的相关内容纳入统一的隐私政策，与其他个人信息处理事项一并告知个人信息主体，这样获取同意的方式被监管者视为“概括同意”。而《二审稿》第 39 条特别要求企业明确告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息种类和行使权利的方式等事项，并取得**单独同意**。具有跨境传输个人信息需求的企业应据此调整告知和获取同意的方式，例如通过单独的页面或弹窗告知用户个人信息出境详情并获取授权，在员工入职前要求其签署专门的个人信息出境同意书等。

2. 开展个人信息出境自检

目前大量企业，尤其是跨国企业已经开展个人信息出境活动，待《个人信息保护法》和相关配套法规正式生效后，该等活动均应按照规定通过安全评估、通过个人信息保护认证或签署标准合同。考虑到实践中相关活动的复杂性，企业可能难以在短时间内梳理个人信息出境、出境必要性、获取授权同意、实施安全保障措施、保障个人信息主体权益、监督合同履行、接收方安全保障能力、接收国家或地区的法律环境等情况，进而无法按时履行法定义务。建议企业尽早对目前的个人信息出境相关活动开展自查，完善相关制度和流程(尤其是提前建立风险评估程序，对个人信息出境的“合法性、正当性和必要性”进行判断，并依据已经生效和可能生效的数据流通规则调整企业的个人信息出境实践)，对尚未开展的个人信息出境进行个人信息安全影响评估，以降低跨境传输个人信息的法律风险。

尤其值得注意的是，由于标准合同关涉接收者的权利和义务，要求接收方承担保护个人信息主体权益的责任。建议企业尽早在该等条款框架内与交易相对方就个人信息提供的问题进行协商谈判，以减少相关规定和标准合同的正式出台和适用对目前业务和交易的影响。

3. 关注特殊领域的单行监管要求

尽管总体的个人信息出境限制尚未明晰，但我国目前已经在某些领域的立法中对个人信息出境做出了专门规定，例如医疗行业中的人口健康信息、健康医疗大数据和人类遗传信息，金融行业中的个人金融信息、证券业务活动中有关的文件和资料等。相关企业除关注一般个人信息出境义务外，还应严格遵守并密切关注所属行业要求，为相关企业、组织和机构提供运维、管理等服务的企业也应注意法律法规对其个人信息存储、出境的限制，防范合规和合同风险。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

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	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	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