

我国个人信息出境认证制度浅析

作者：杨迅 | 李依然 | 郑学易

2025 年 10 月 14 日，国家网信办、国家市场监督管理总局联合发布了《个人信息出境认证办法》（“《认证办法》”），明确了个人信息出境认证（“出境认证”）的适用情形、申请方式、认证要求等内容，标志着《个人信息保护法》（“《个保法》”）明确的数据出境安全评估、个人信息保护认证、个人信息出境标准合同这三项出境制度设计的全面落地，以及我国数据跨境流动制度体系的全面建立。

1. 出境认证制度概览

出境认证制度是我国《个保法》下个人信息跨境流通的三条路径之一，也是唯一一条，至少表面上，非政府介入的路径。

(1) 出境认证是《个保法》下数据出境的合规路径之一

出境认证是《个保法》下的个人信息出境合规路径之一。根据《个保法》第 38 条的规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定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。

这些年，随着《数据出境安全评估办法》、《个人信息出境标准合同办法》以及《促进和规范数据跨境流动规定》等法律法规相继出台，我国已经建立起了个人信息出境制度的基础框架，并形成了较为完整的法律法规体系。《认证办法》在上述法律法规的基础上，进一步细化了出境认证的具体实施规则和流程。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

那什么是“个人信息保护认证”呢?根据《认证认可条例》第2条第1款,“认证”指“由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动。”根据《认证办法》第3条,出境认证是指按照《个保法》相关规定,“由依法取得个人信息保护认证资质的专业认证机构,证明个人信息处理者向中华人民共和国境外提供个人信息等个人信息处理活动符合相关法律、行政法规、部门规章、标准、技术规范的合格评定活动。”

(2) 出境认证的发展历史

自《个保法》生效以来,国家网信办等各部门开展了出境认证制度的探索,相继颁布了一系列政策文件:

- (a) 2022年6月,信安标委发布《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(TC260-PG-20222A)》(“《认证规范 1.0》”),为落实《个保法》、建立个人信息保护认证制度提供认证依据。
- (b) 2022年11月,国家网信办以及市场监督管理总局发布《关于实施个人信息保护认证的公告》及附件《个人信息保护认证实施规则》,对个人信息保护认证规则进行了整体构建,并明确规定开展跨境处理活动的个人信息处理者,其认证依据应包括《认证规范 1.0》。
- (c) 2022年12月,信安标委发布《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)(TC260-PG-20222A)》,对《认证规范 1.0》进行了进一步修订和完善。
- (d) 2025年8月,市场监管总局(国家标准委)批准发布《数据安全标准 个人信息跨境处理活动安全认证要求(GB/T 46068—2025)》(“《认证要求》”)。这是我国个人信息跨境安全管理领域的首项国家标准,规定了跨境处理个人信息时相关方应遵守的基本原则、基本要求和个人信息主体权益保障要求,为规范个人信息跨境处理活动提供了依据。在效力层级方面,国家标准的效力高于实践指南。
- (e) 2025年10月,《认证办法》正式出台,补齐了我国数据出境法律法规体系中在出境认证方面的部门规章空缺。

(3) 域外视角

从国际实践观之,认证制度在个人信息出境中亦发挥了重要作用。例如,日本、新加坡等国家均采用了亚太经合组织推出的全球跨境隐私规则(Global CBPR)作为跨境数据传输的手段。其次,以欧盟为例,GDPR第46条要求数据控制者或处理者在向第三国或国际组织进行个人信息传输时必须提供适当的安全保障措施,其中就包括GDPR第42条规定的认证机制。为此,欧盟相继发布了《关于GDPR第42、43条的认证和识别认证准则的指南》、《关于认证作为跨境传输工具07/2022指南》(“《认证作为跨境传输工具指南》”)、《有关认证和认可程序问题的回应》等文件以构建欧盟境内的个人信息认证制度。比较中欧两地就出境认证方面的有关制度,其存在如下差异:

- (a) 适用范围: 在 GDPR 下, 一个数据处理活动是否构成跨境传输必须满足三个必备要素: (1)某控制者或处理者的处理行为受 GDPR 管辖; (2)控制者或处理者(发送方)通过传输或其他方式将受其处理的个人信息提供给另一个控制者、共同控制者或处理者(接收方); (3)接收方位于第三国或是一个国际组织。因此, 如果在境内缺乏相应的发送方, 就不构成数据跨境传输; 但在中国的出境认证制度下, 根据《认证要求》第 3.7 条, “符合《个保法》第三条第二款情形, 在境外处理境内自然人个人信息的活动”亦可申请认证, 也就是说, 即便不存在境内实体, 境外主体跨境直接收集个人信息的场景亦构成数据出境, 进而可适用跨境认证。
- (b) 申请认证主体: 根据《认证作为跨境传输工具指南》, 在 GDPR 的法律框架下, 申请跨境认证的主体为在第三国的进口方, 而对于出口方来说, 若其意图选择认证作为跨境传输工具, 则需要检查进口方是否取得认证, 且认证是否有效且未过期, 是否涵盖了要进行的具体传输。但在中国, 根据《认证办法》第 7 条, 申请认证的主体为境内的个人信息处理者, 或者境外的个人信息处理者在境内设立的专门机构或者指定代表, 即是由境内主体进行出境认证申请。
- (c) 认证标准: 根据《认证作为跨境传输工具指南》, GDPR 下跨境认证的标准尤其关注对第三国立法的评估、在国家立法妨碍遵守作为认证一部分的承诺的情况下的程序和行动、处理第三国当局的数据访问请求等内容, 从本质上, 欧盟数据跨境传输机制的核心关注点在于境外接收方所在国能否提供与欧盟同等的数据保护水平(特别是在公共当局对数据访问请求方面), 以及若无法提供同等的数据保护水平, 接收方是否采取了补充措施以降低相应风险。而中国的出境认证制度则更加关注境内处理者与境外接收方之间具有拘束力的文件、设置个人信息保护负责人与个人信息保护机构、遵守统一的个人信息跨境处理规则及进行事前个人信息保护影响评估等内容。

值得一提的是, 截至目前, 根据 EDPB 官网的公开信息查询, 目前欧盟境内已注册登记的认证机制(例如 Europrivacy)均无法作为“跨境传输工具的认证”, 这意味着欧盟将认证作为个人信息跨境传输的工具的制度仍未实质落地。

2. 出境认证的适用范围

个人信息出境认证途径适用于不需要经过安全评估(且不属于豁免场景)的个人信息出境, 尤其适用于境外信息处理者直接处理中国境内个人信息。

(1) 适用场景

在我国个人信息出境的监管实践中, 个人信息出境的定义不仅包含: 境内处理者将数据传输至境外; 以及个人信息虽存储在境内, 但境外接收方有权访问存储于境内的个人信息这两个典型场景; 亦包括境外个人信息处理者直接采集和处理境内个人信息的场景, 即跨境直采场景。

实践中, 由于在跨境直采场景下缺乏境内的个人信息处理者, 如何签署以及履行标准合同备案程序等问题存疑。部分地方网信办要求境外处理者与由其在境内设立的专门机构或者指定代表协助签署标准合同, 并向属地网信办进行标准合同备案。

这一具有中国特色的监管思路亦体现在了出境认证制度中, 《认证办法》第 7 条明确规定“个人信息处理者通过认证方式向境外提供个人信息的, 应当向专业认证机构申请出境认证。中华人民共和国境外的个人信息处理者申请出境认证的, 应当由其在境内设立的专门机构或者指定代表协助进行申请。”

(2) 适用条件

根据《认证办法》第 5 条, 个人信息处理者通过出境认证的方式向境外提供个人信息的, 应当同时符合下列情形:

- (a) 非关键信息基础设施运营者;
- (b) 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;
- (c) 向境外提供的个人信息, 不包括重要数据。

总体而言, 出境认证的适用范围与个人信息出境标准合同备案一致。

3. 出境认证的实施和效力

开展出境认证的, 应当依照以下规则。

(1) 专业认证机构

根据《认证办法》第 7 条, “个人信息处理者通过认证方式向境外提供个人信息的, 应当向专业认证机构申请出境认证。”而根据《认证办法》第 12 条, 开展出境认证的专业认证机构须经国家市场监督管理总局批准个人信息保护认证资质并且及时向国家网信部门办理备案。从要求的备案材料来看, 认证机构的规格还是比较高的, 实操中, 目前具备专业资质的机构包括中国网络安全审查认证和市场监管大数据中心¹。

(2) 基本程序

根据《认证办法》第 8 条第 1 款, 专业认证机构按照认证基本规范、个人信息保护认证规则开展出境认证。即出境认证的具体工作主要依据上文所述的《认证要求》、《个人信息保护认证实施规则》, 基本程序包括认证委托、技术验证、现场审核、认证结果评价和批准、获证后监督, 认证的具体事项包括对以下方面的考察:

¹ <https://www.isccc.gov.cn/>

- (a) 个人信息处理者和境外接收方在跨境处理个人信息时落实合法、正当、必要和诚信原则，公开、透明原则，同等保护原则，责任明确原则。
- (b) 个人信息处理者和境外接收方签订合同或其他具有法律约束力和可执行的文件，保障个人信息主体权益。
- (c) 个人信息处理者和境外接收方均设有履行个人信息保护职能的机构、指定个人信息保护负责人，约定并遵守共同的个人信息跨境处理规则。
- (d) 个人信息处理者针对跨境处理活动开展个人信息保护影响评估。
- (e) 个人信息处理者和境外接收方承认并落实个人信息主体享有的各项权利，为行使相关权利提供便利条件。
- (f) 个人信息处理者和境外接收方明确各自义务和责任，包括落实告知义务和单独同意，落实境外接收方经营情况变化、所在地法律法规变化或执法要求导致的通知和保护义务，不得超出约定范围处理个人信息，确保密码技术符合相关标准，发生安全事件后的补救措施、通知和报告等。

根据《认证办法》第 8 条第 2 款，出境认证的证书有效期为 3 年，证书到期如需继续使用的，个人信息处理者应当在届满前 6 个月提出认证申请。

(3) 认证的作用和持续监督

作为数据出境的合规路径之一，个人信息处理者通过出境认证并不意味着一劳永逸。在有效期内，认证机构对认证证书状态进行信息报送，对已获认证的个人信息出境情况持续监督。

根据《认证办法》第 9 条第 1 款，专业认证机构应在出具认证证书或者认证证书状态发生变化后及时向全国认证认可信息公共服务平台报送个人信息出境认证证书相关信息。进一步地，根据《认证办法》第 10 条第 1 款，专业认证机构发现获证个人信息处理者存在个人信息出境情况与认证范围不一致等情形，不再符合认证要求的，应当暂停其使用直至撤销相关认证证书。例如，此前已获认证的珠海澳科大科技研究院的认证证书据查询目前已被撤销。

此外，根据《认证办法》第 13 条，国家市场监督管理总局和国家网信部门对个人信息出境认证活动进行监督，开展定期、不定期检查，并且对认证过程、认证结果进行抽查，对专业认证机构进行抽查和评价。这些要求强化了专业认证机构的业务水平、专业责任与公信力，也有利于鼓励符合条件的企业利用出境认证制度提升企业合规水平。

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

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

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

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

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

伦敦

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

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2025