

选项越多选择越困难?个人信息出境选标准合同还是认证?

作者: 潘永建 | 朱晓阳 | 邓梓珊 | 左嘉玮

想必大家都已经熟知我国个人信息出境的三条政府监管路径,即数据出境安全评估、个人信息出境标准合同,以及个人信息保护认证。其中,安全评估与标准合同均已有位阶较高的法规予以明确规定(《数据出境安全评估办法》及《个人信息出境标准合同规定》均为国家互联网信息办公室(“网信办”)的部门规章),而有关认证的法规却迟迟没有出台。2022 年 11 月 4 日,网信办与国家市场监督管理总局曾联合发布《关于实施个人信息保护认证的公告》,但这仍然没有明确认证的法律地位。在近日,网信办终于发布了《个人信息出境个人信息保护认证办法(征求意见稿)》(“《认证办法》”),对出境认证的适用情形、评估内容及操作流程等进行了细化和完善。本文旨在梳理《认证办法》的核心内容,并分析在个人信息出境路径中,选择标准合同备案还是认证机制的主要考量。

一. 个人信息出境活动的认定

《认证办法》沿用了《数据出境安全评估申报指南(第二版)》和《个人信息出境标准合同备案指南(第二版)》中对于个人信息出境活动的界定,明确以下三种典型出境情形:

- 个人信息处理者将在境内运营中收集和产生的个人信息传输至境外;
- 个人信息处理者收集和产生的个人信息存储在境内,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》(“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等其他个人信息处理活动。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

值得注意的是第三类情形，根据个保法的域外适用原则，在满足“向境内自然人提供产品或服务”或“分析、评估境内自然人行为”两种情形之一时，个人信息处理活动将直接受到个保法的规制。《认证办法》进一步明确，相关境外处理者在对境内自然人个人信息开展处理活动之前，还需就“自境外收集数据”的行为完成个人信息出境的相关合规程序。如选择适用认证，应由境外处理者在境内设立的专门机构或者指定代表协助进行申请。

二. 认证的适用条件

与《促进和规范数据跨境流动规定》第八条的规定保持一致，企业在选择认证作为个人信息出境的合规路径时，需满足以下三个条件：

- 企业未被认定为关键信息基础设施运营者；
- 不涉及出境重要数据；
- 当年累计向境外提供 10 万人以上、不满 100 万人普通个人信息(不含敏感个人信息)；或者当年累计向境外提供不满 1 万人敏感个人信息。

在选择认证路径前，建议企业对自身个人信息出境活动进行全面梳理，包括明确涉及的业务场景、数据的类型以及出境规模。特别是对于出境数据是否涉及重要数据，应密切关注相关主管部门发布的政策文件，以确保符合认证的适用条件。

三. 认证的评估内容

《认证办法》提出了六大方面的评估内容，与标准合同备案的评估要求有一定重叠，具体如下表：

认证	标准合同备案
(一)个人信息出境的目的、范围、方式等的合法性、正当性、必要性；	(一)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；
(二)境外个人信息处理者、境外接收方所在国家或者地区的个人信息保护政策法律和 网络和数据安全环境 对出境个人信息安全的影响；	(五)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；
(五)个人信息处理者、境外接收方的 组织架构、管理体系、技术措施 能否充分有效保障数据安全和个人信息权益；	(三)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；
(四)个人信息处理者与境外接收方订立的有法律约束力的协议是否约定了个人信息保护的义务；	(四)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；

(三)境外个人信息处理者、境外接收方的个人信息保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求;	(二)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;
(六)专业认证机构根据个人信息保护认证相关标准认为需要评定的其他事项。	(六)其他可能影响个人信息出境安全的事项。

两者的主要区别包括:

- 认证区分了“境外个人信息处理者”和“境外接收方”两类角色, 并且在第(四)项中, 仅要求评估个人信息处理者与境外接收方之间订立的协议。按此理解, 如果认证对象为“境外个人信息处理者”, 则无需额外签署跨境传输相关协议;
- 认证的第(五)项中, 要求同时对个人信息处理者和境外接收方的“组织架构、管理体系、技术措施”进行评估, 而标准合同备案侧重于评估境外接收方“履行义务的管理和技术措施、能力”, 对个人信息处理者的管理能力等没有特别要求。

四. 信息公开与持续监督

《认证办法》强调认证过程的透明度和对于认证结果的持续监督。认证机构需在颁发认证证书后的五个工作日内, 将相关信息报送至全国认证认可公共信息平台(<https://cx.cnca.cn/>)。

此外, 认证机构需建立持续监督机制, 确保认证主体在认证有效期内持续符合标准。一旦发现认证主体在证书有效期内不再符合认证要求的, 认证机构可以暂停、撤销认证证书, 并将相关情况予以公布。国家网信部门和相关监管部门也将对获证主体进行监督管理, 并对存在问题的企业采取相应措施。

五. 认证与标准合同备案如何选择?

由于大多数企业不会触发数据出境安全评估的高门槛要求, 标准合同备案和个人信息保护认证将成为企业实现个人信息出境的主要合规路径。那么, 企业在考量到底选择标准合同备案还是个人信息保护认证时, 应当考虑哪些因素呢? 以下我们列出了两者的对比, 供企业判断选择:

维度	认证	标准合同备案
评估内容	认证的评估内容更为广泛, 需要同时评估个人信息处理者和境外接收方的组织架构、管理体系、技术措施。境内企业需要在内部流程优化、管理机制健全以及技术能力建设方面投入更多的资源和精力。	标准合同备案重点评估境外接收方的技术、管理措施是否可以履行标准合同所规定的义务以及保护出境个人信息安全。 备案对于境内企业的组织架构和内部管理体系关注较少, 主要集中在数据“出境后”的安全保障。

公开性	认证通过后, 企业的认证证书将被公开披露, 能够在一定程度上证明企业的数据合规能力, 对于希望提升客户信任和行业声誉的企业来说是一个加分项。	标准合同备案的信息不对外公开, 缺乏类似的背书效应。但企业也可以选择将备案的通知结果提供给相关需求方。
有效期	根据《个人信息保护认证实施规则》第 5.1 条, 认证证书的有效期为三年。企业需要在证书到期前六个月提出续期申请, 经认证机构审核后方可延续认证。	标准合同备案的有效期由合同双方协商确定。在实践中, 备案合同的有效期通常具有更大的灵活性, 甚至可以约定为长期有效。
费用	认证需要通过指定的专业认证机构进行评定, 会产生一定的费用。例如, 根据中国网络安全审查认证和市场监管大数据中心 (CCRC) 公布的收费标准, 认证费用包括以下项目: - 申请费: 18,000 元/认证单元; - 评定注册费: 24,000 元/认证单元; - 审核/验证费: 6,000 元/人日; - 年金: 50,000 元/年认证单元; - 技术验证费: 另行计算。	标准合同备案由省级网信部门负责审查, 无需企业支付费用。
条款灵活性	认证允许企业与境外接收方协商出境条款内容, 因此适用于境外接收方立场较为强硬、企业自身谈判能力有限的情形。	标准合同备案要求双方严格遵循国家网信部门发布的标准合同模板, 条款不可修改。在实践中, 部分境外接收方可能因对部分条款(如责任划分)存在异议而拒绝签署。

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



朱晓阳
+86 21 3135 8683
nigel.zhu@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