个人信息出境认证机制展望
——以《个人信息跨境处理活动安全认证规范》为起点

作者：潘永建 | 朱晓阳 | 吴若蘅

除法律规定适用个人信息出境数据安全评估的情形外，《个人信息保护法》将“标准合同”或“个人信息保护认证”作为个人信息出境的前提条件。国家网信办于 2022 年 6 月公布了《个人信息出境标准合同》的草案，为个人信息通过标准合同出境拉开了序幕。关于个人信息保护认证应当如何进行，相关法律法规却迟迟未见出台。

针对个人信息出境认证，全国信息安全标准化技术委员会(“**信安标委**”)于 2022 年 6 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(TC260-PG-20222A)》(“**《认证规范》**”)，对“个人信息跨境处理”涉及的认证提出了相应的指引。信安标委此后又于 2022 年 11 月 8 日发布了《认证规范》2.0 版的征求意见稿。根据《认证规范》，其旨在“为认证机构对个人信息处理者的个人信息跨境处理活动开展认证提供依据，也为个人信息处理者规范个人信息跨境处理活动提供参考”。值得注意的是，国家市场监督管理总局及网信办于 2022 年 11 月 18 日发布了《个人信息保护认证实施规则》(“**《认证规则》**”)，其中规定“对于开展跨境处理活动的个人信息处理者，还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求”。

《认证规则》及《认证规范》的出台无疑将个人信息出境认证机制向前推进了一大步，但也要看到《认证规则》将《认证规范》纳入“个人信息跨境处理”认证的同时，也引发了对《认证规范》的法律效力、适用范围与主体、认证对象、认证具体流程、境外接收方的法律责任、认证机制简化等诸多规范和实践问题的思考。因此，我们结合法律法规及自身经验，对《认证规范》的效力、适用范围及适用主体等进行解读，同时也列出《认证规范》中尚未明确的问题，展望个人信息出境认证机制的未来趋势。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

1. 法律效力、适用范围与主体

首先，就《认证规范》的法律效力而言，其属于由信安标委发布的技术规范，本身并没有法律强制力。尽管如此，根据《中华人民共和国认证认可条例》，“认证”是指“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”。因此，《认证规范》可以成为相关认证机构对“个人信息跨境处理”活动进行认证时援引的技术规范，从而在个人信息跨境处理认证中具有法律效力。

然而，需要注意的是，《认证规范》中“个人信息跨境处理”的表述与《个人信息保护法》中“个人信息跨境提供”的表述并不一致。因此其内涵是否一致值得研究。根据《认证规范》，其适用范围包括: (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”；及(2)“《个人信息保护法》第三条第二款规定的境外个人信息处理者(的个人信息跨境处理活动)”。上述两种情形中，第(1)种情形属于跨国集团内部的个人信息跨境提供，属于《个人信息保护法》下个人信息跨境提供的一种；第(2)种情形则针对的是“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”。对此我们认为可能有两种解释，第一种是个人信息已经完成从中国出境后，在境外的处理活动；第二种是境外个人信息处理者从境外直接收集、处理中国境内个人信息的个人信息跨境处理活动。但无论是上述哪种解释，由于缺乏境内的数据出境主体，似乎都难以解释为《个人信息保护法》下的“个人信息跨境提供”。因此，与其将第(2)种情形解释为个人信息跨境提供情境下的个人信息保护认证，我们认为更合理的解释是《认证规范》新创设了针对“境外个人信息处理者直接处理境内个人信息”这一情形的认证，但这与《个人信息保护法》下的个人信息跨境提供认证并无关联。

由此可见，对于《个人信息保护法》下的“个人信息跨境提供的认证”，《认证规范》只规定了这其中涉及跨国集团内部个人信息跨境提供的部分，相当于限缩了《个人信息保护法》下的认证范围。相应地，后续有待进一步立法的问题便是，“个人信息跨境提供认证”是否仅限于跨国集团内部，抑或是还会有针对非跨国集团的、适用于其他一般场景的个人信息跨境提供认证规则。

综上，我们认为《认证规范》属于《个人信息保护法》下针对“个人信息跨境提供”进行认证所依据的技术规范，但针对“个人信息跨境提供”而言，认证机制的适用范围及适用主体是否仅限于跨国集团内部，目前仍尚不明确。

2. 思考与展望

新修订的《认证规范》无疑从更明晰的定义、适用主体和范围、基本原则、个人信息处理者和境外接收方的责任义务、响应个人信息主体保障权益等各方面综合考量，为企业的个人信息出境认证提供了更明确的指示和要求。但如上所述，《认证规范》在适用范围、适用主体，以及与《个人信息保护法》下“个人信息跨境提供”认证机制的衔接等方面仍然存在一些有待明确的问题。下文中我们尝试为读者阐明这些问题，并提出我们对于认证机制未来发展的思考和展望。

1) “个人信息跨境处理活动”的含义

鉴于《认证规范》及《认证规则》中提出的“个人信息跨境处理活动”与《个人信息保护法》等法律中的表述不一致，且没有明确的定义，我们认为有必要对“个人信息跨境处理活动”的定义予以明确。

结合上述分析，基于目前《认证规范》的内容，似乎可以将“个人信息跨境处理活动”解释为“个人信息跨境提供”以及“境外个人信息处理者直接收集境内个人信息”两种情形，其中对于“个人信息跨境提供”的认证的法律依据为《个人信息保护法》，而对于“境外个人信息处理者直接收集境内个人信息”的认证不落入《个人信息保护法》的规定，其法律依据为《认证规则》。

无论后续立法或执法机构是否会按照我们对“个人信息跨境处理活动”的上述解读去进行定义，我们认为赋予“个人信息跨境处理活动”明确的外延和内涵，将更有助于有个人信息出境需要的主体选择合适的个人信息出境的法律路径。

2) 认证机构、流程及材料

《认证规范》对于个人信息跨境处理活动的认证规范做出了详细的规定，但从企业的角度，更为关心的问题无疑是认证的具体程序。例如，应该向哪个(些)认证机构提交认证申请、认证的具体流程和时间限制，以及认证需要提交哪些申请材料。

对于认证机构，《认证规则》及《认证规范》均未予以明确。《认证规范》中提及《认证规范》的制定得到了中国网络安全审查技术与认证中心(CCRC)的技术支持，而且 CCRC 也是目前网信办开展数据出境安全评估的技术评测方，因此，我们认为个人信息跨境处理活动的认证有可能会委托 CCRC 进行。此外，认证工作的常规主管机构为国家认证认可监督管理委员会(CNCA)，且 CNCA 已经认定并发布了认证机构的名录列表(参见认证机构信息列表)[1]，因此未来也不排除将认证工作交由 CNCA 指定的认证机构进行。

认证的材料及认证所需的法定时限也有待进一步的明确。由于《认证规范》中明确对“有法律约束力的协议”提出了规范要求，将来出境方与境外接收方就个人信息跨境处理活动签署的个人信息出境协议(是否需要采用网信办公布的标准合同有待明确)或将会作为认证申请材料的重要部分。

3) 认证对象

目前《认证规则》及《认证规范》尚未明确的另一个问题是，认证的对象究竟是“个人信息跨境处理活动”，抑或是出境或境外接收个人信息的主体。

[1] 认证机构信息列表，http://cx.cnca.cn/CertECloud/institutionBody/authenticetionList.

如果认证的对象是“个人信息跨境处理活动”，那么认证的范围将会相对较为狭窄，即便是跨国集团内部的数据出境活动，其出境个人信息的目的、范围、类型和方式也不是一尘不变的，如果仅仅针对“处理活动”进行认证，那么很有可能导致后续处理活动发生变化后，需要重新进行认证。

企业更期待看到的应当是对于出境主体和/或境外个人信息接收主体的认证，即认证是对个人信息出境方和/或境外接收方的个人信息出境合规及个人信息安全保护能力的证明。也就是说，即使其出境/接收的个人信息范围、类型等始终在变化，经过认证的主体仍然可以自由地在遵守中国法律的前提下，进行个人信息出境/接收行为。 如此，可适当减轻企业的合规负担，从而提升企业进行认证的积极性。

4) 认证有效期

根据目前的法律草案，除非合同涉及的出境情形发生重大变化，否则标准合同备案后将长期有效。对于认证而言，我们认为将会采取相同的机制，即除非认证的“个人信息跨境处理活动”，或认证的对象发生重大变化，个人信息跨境提供的认证也将会是长期有效的状态。

5) 认证与标准合同的关系

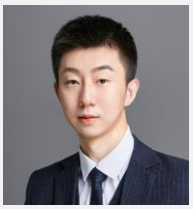
就个人信息跨境提供而言，认证与标准合同并列个人信息跨境提供的法律路径。但除非这两种路径的复杂性、有效性、成本等完全相同，否则企业没有理由不选择更容易、成本更低的路径。

从目前《认证规范》对于“有法律效力的协议”的要求来看，很有可能会要求申请认证的主体提交境内外双方签署的出境协议(即使不是标准合同，也不会有太大的区别)。意即企业如果通过标准合同出境个人信息，仅需签订合同，而如果通过认证出境个人信息，除标准合同外，还需要履行其他的认证手续。若如此，除非认证机制在其他方面有优于标准合同之处，出境方恐难说服境外接收方配合进行个人信息出境认证。

我们认为，相较于标准合同仅能与单个的境外接收方一对一签署，且合同中能约定(预见)的数据出境场景和类型也比较固定，认证的机制可以是相对比较灵活的。例如，认证不仅可以针对个人信息跨境提供的行为，也可以针对跨境提供的提供方和接收方主体。如果可以针对主体进行认证，比如对某一境外接收方进行认证，只要已经证明其具有符合中国法律要求的数据安全保护能力，此后其从其他境内主体接收数据，或者境内主体向其传输的个人信息范围或类型发生变化，不需要再履行认证或者其他的个人信息跨境提供义务。此将大大提高认证机制对于个人信息出境方及境外接收方的吸引力，促使企业选择认证作为个人信息出境的法律路径。

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	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