

个人信息跨境处理活动安全认证制度的建立 ——兼谈认证制度实施对金融机构的启示

作者：杨迅 | 夏雨薇

个人信息保护认证路径悄然落地。与“标准合同”和“网信办的安全评估”不同，认证制度似乎着力于对跨国集团整体的个人信息保护的技术能力和管理能力的审查。这可以作为需要多条线、多迂回和境内外同时处理境内客户信息的跨国金融机构的一项值得考虑的选择。

近日，中国网络安全审查技术与认证中心(“CCRC”)上线了“个人信息保护认证业务管理系统”并公开了《个人信息保护认证申请书》，成为了《个人信息保护认证实施规则》(“《认证规则》”)颁布后的首个被认可开展个人信息保护认证活动(“认证活动”)的认证机构。认证机构的确认意味着个人信息保护与跨境处理认证制度(“认证制度”)的落地，也意味着个人信息出境的三条路径，除《个人信息出境标准合同规定》尚在征求意见外，已经初步呈现。

对于跨国公司，尤其是跨国金融机构，存在大量集团内部信息共享的情形，也存在不少境外机构直接收集境内客户信息的安排。认证制度将在很大程度上有助于这些情形和安排的合规。

一. 认证制度一览

认证制度首次出现在《个人信息保护法》。根据该法第 38 条，“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，应该……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……”从而，认证活动成为个人信息出境的三条路径之一。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

此后,2022 年 11 月 4 日,国家市场监督管理总局和国家互联网信息办公室联合颁布了《认证规则》,在行政规章层级细化了认证活动的实施程序;2022 年 12 月 16 日,全国信息安全标准化技术委员会秘书处发布正式版《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》(“**认证规范 2.0**”)对认证活动的适用、主体和认证要求作出规定。

近日,CCRC 被指定为首家有权开展认证活动的机构,标志着认证制度全面落地。

认证活动的适用

《认证规范 2.0》颁布后,对认证活动适用的情形不设特殊限制。而且,《认证规范 2.0》并未排除适用“网信部门安全评估”的情形,其第 1 条“适用情形”规定:《认证规范 2.0》是“对个人信息跨境处理活动进行个人信息保护认证的认证依据,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。”换言之:

- 认证活动可以成为满足《个人信息保护法》第 38 条下的个人信息出境的合法途径之一;和
- 对于适用“标准合同”或“网信办安全评估”路径的信息出境行为,认证活动也可以成为个人信息跨境处理的合规性和安全性的参考。

认证活动的申请主体

在《认证规范 2.0》下,只要具有“合法的法人资格”,“正常经营且具有良好的信誉、商誉”的主体,都可以成为认证活动的申请主体。《认证规范 2.0》尤其指出以下数据出境情形下的认证活动申请主体:

- **跨国集团内部的个人信息传输。**由境内的一方作为认证主体,并承担法律责任。
- **境外个人信息处理者直接跨境处理个人信息。**由该境外个人信息处理者在境内设立的专门机构或指定代表申请认证,并承担法律责任。

本条是对《个人信息保护法》第 53 条中境外个人信息处理者应“在中国境内设立专门机构或者指定代表,负责处理个人信息保护相关事务,并将有关机构的名称或者代表的姓名、联系方式等报送监管部门”之义务的呼应。也是首次明确指明境外个人信息处理者“在境内设立的专门机构或指定代表”这一项职能。但是,不清楚的是该“境内设立的专门机构或指定代表”所承担的“法律责任”的范围到底有多大,是仅仅对认证活动申请“承担法律责任”,还是对后续所有境外个人信息处理者处理境内个人信息的活动负责。

认证要求

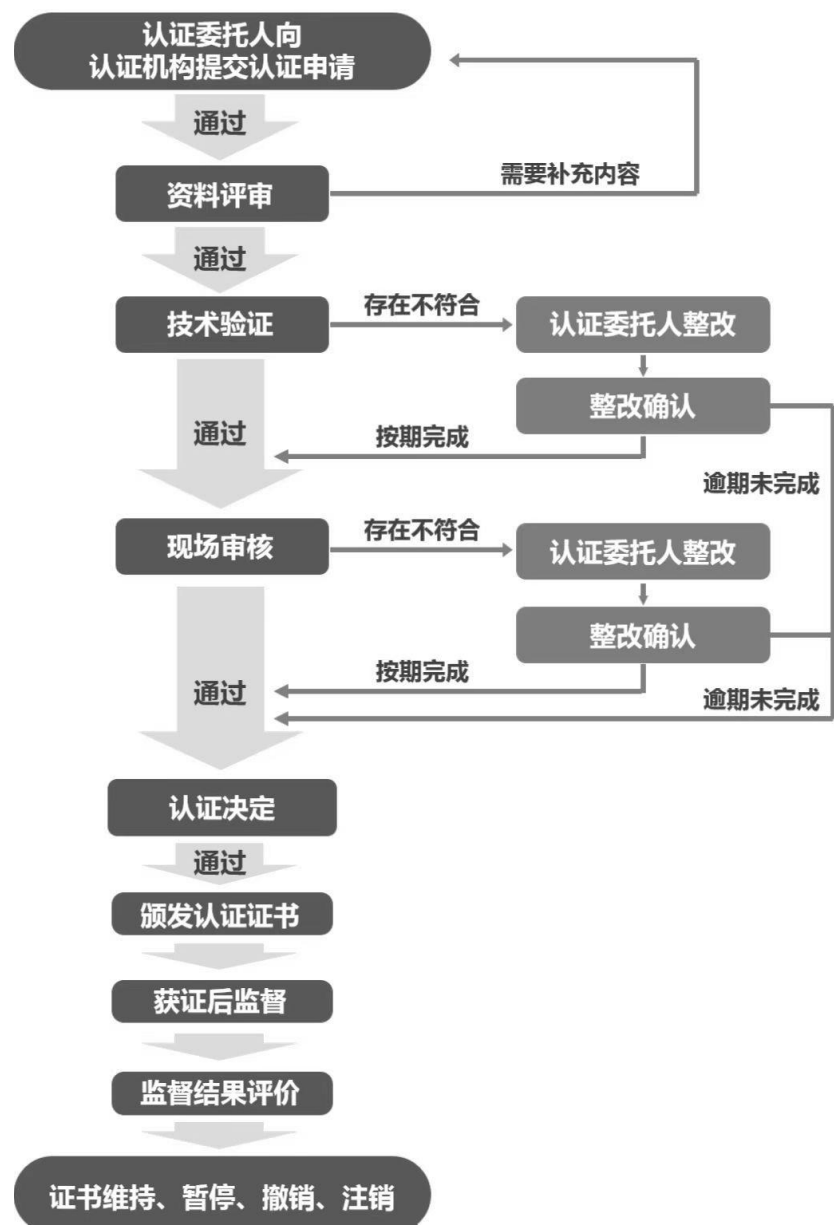
根据《认证规则》,开展认证活动,主要考察跨境个人信息传输对以下规范的合规性:

- GB/T 35273《信息安全技术 个人信息安全规范》,这是个人信息保护领域全方位的行为规范。
- 《认证规范 2.0》,作为针对跨境个人信息传输的行为规范,其给跨境个人信息传输设定一系列要求,包括(1) 签订具有法律约束力的文件; (2) 任命个人信息保护负责人、建立个人信息保护机

构; (3) 建立个人信息保护规则; (4) 进行个人信息保护影响评估 (5) 建立个人信息主体权益保障机制等。

二. 认证流程

国家认监委公布其认证活动的流程如下:



三. 认证要点

CCRC 在其公布的《个人信息保护认证申请书》中指出了认证活动对个人信息处理者和处理活动考察的内容, 其要点如下:

12 个月内未发生过个人信息安全事件

《个人信息保护认证申请书》要求申请方承诺，近 12 个月内未发生重大个人信息安全事件。换言之，认证活动的申请方，必须保持良好的个人信息保护和网络安全记录，避免重大个人信息安全事件的发生。

提供数据分级分类目录

《个人信息保护认证申请书》要求申请方参考相应标准，以指定格式披露个人信息处理业务和跨境处理所涉的数据分级分类目录。

对数据进行分级分类保护，在《网络安全法》下对网络运营者的要求中初步体现，在《数据安全法》下正式确立，同时也涵盖在《个人信息保护法》下个人信息处理者的合规义务中，数据分级分类保护制度，更是保护信息安全，规范数据处理行为的基础。

特别是，CCRC 也在《个人信息保护认证申请书》中明确数据目录的变更可能构成影响认证有效性的变更，CCRC 或需重新审批，这也对数据分级分类工作的准确性、严谨性和稳定性提出更高要求。

技术验证和入场审核

技术验证和入场审核是个人信息保护认证的必要环节。但对境外的个人信息处理者而言，如何实现该要求仍需要进一步的实务探索。如果确需进行的，是否是由其在境内的专门机构或指定代表进行技术验证与入场审核，对境内代表的审核如何能够核验境外的个人信息处理者的保护能力和技术资质？以上问题还有待澄清。

与个人信息相关的业务流披露

《个人信息保护认证申请书》要求申请方对所有个人信息跨境处理活动的接收方、组织机构图与跨境业务流程进行描述。对于存在多种场景信息传输的金融机构而言，跨境处理信息的主体较多，需考虑对相应的数据链路进行梳理与整合，精简集团内部分冗余的数据流。

四. 认证活动对跨国金融机构的启示

认证制度的建立，对跨国金融机构而言，可能是个利好消息。因为，这意味着跨国金融机构繁复的个人信息出境多了一条可选择的途径。

跨国金融机构个人信息出境场景和认证制度的适用

跨国企业，尤其是跨国金融机构，在个人信息的跨国传输方面往往具有如下特点：

- 多线条、多迂回的个人信息出境路线。

跨国公司集团往往采取 IT 资源的全球部署, 实现内部资源和信息集团内共享。比如, 很多境内金融机构(比如证券、基金公司等)将其人力资源有关信息汇总给一家非监管的服务公司, 服务公司可能使用部署于新加坡的系统(比如 Workday)开展人力资源管理, 而该系统的后台权限可能位于印度, 而为了风控目的, 部分人力资源信息可能被纽约总部使用。于是乎, 某些员工个人信息在境内外迂回, 到底什么时刻, 由哪一个实体出境难以辨明, 在集团成员中的流转路径错综复杂。

在这种情况下, 单独的点对点的出境合同和网信办安全评估, 可能难以实施, 也不能准确反映信息出境的风险全貌。而以集团为整体的认证, 则能更好地解决这个问题。

- 境内外共同处理个人信息。

很多跨国公司和金融机构的境内外实体同时为客户在境内外分支机构提供服务。比如, 企业客户可能寻求跨国证券公司同时在境内外开展证券融资活动。在这种情况下, 境内客户的信息, 包括联系人和受益人信息需要提供给该证券公司的境内外分支机构, 这就可能同时存在跨国金融机构的境外主体直接向境内收集个人信息和境内主体向境外主体传输个人信息的场景。

在这种情况下, 单独区分境内客户信息出境的路线, 是由境内实体(受托)转交还是客户直接出境, 可能并没有太多现实的意义, 强行以单独的由境内实体开展数据出境, 或以境外实体收集数据开展评估, 难以反映数据流转及其风险的全貌, 而以集团为整体开展评估的方式, 则更有利于简化安全评估的开展。

认证制度的优势

个人信息跨境处理活动安全认证比标准合同备案更早落地实施, 对于暂未受到网信办监管的处理者而言, 可优先考虑通过个人信息保护认证的方式履行出境义务。正如上述提到的在多线条、多迂回的个人信息出境路线下, 比起与每一个出境的自然人签署标准合同并进行备案的要求, 进行个人信息保护认证的做法更为可行。

而针对需要向网信办申报数据出境安全评估的企业而言(比如大部分面向个人投资者的公募基金)虽申报数据出境安全评估的企业并不要求进行个人信息保护认证, 但如提前完成个人信息保护认证, 也是对自身技术和管理条件的一项强效背书。特别是在目前网信办工作量巨大的情况下, 完成认证是否有助于网信办工作人员对出境申报材料的审核评估, 也值得考虑。

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 2023