短评“认证”：个人信息跨境处理及数据安全管理认证

作者：杨建媛

2022年6月于数据合规领域而言，“认证”是个绕不开的热点话题。月初，数据安全管理认证工作宣告开展、认证实施规则亦已确定；月末，个人信息跨境处理的安全认证规范在征求意见两个月后正式发布。在GDPR体系下，欧盟EDPB起草了首个关于跨境认证的指南（尚未公布文本），为个人数据跨境传输提供了新的工具；卢森堡数据保护监管机构率先采用关于个人数据处理活动合规性的认证机制GDPR-CARPA，并于今日（6月28日）举行启动会议。

研读国内的两个认证规则，其所设定的规则标准不低且具体细致。企业取得认证相当于得到认证机构就管理体系或特定数据处理行为的背书，但为满足相关要求亦需投入相当的合规成本。如何权衡认证收益与合规维护成本？不妨从认证规则入手进行研判。

一、个人信息跨境处理认证

2022年6月24日，全国信息安全标准化技术委员会秘书处发布了《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》（“**《认证规范》**”），以落实《个人信息保护法》（“**《个保法》**”）的个人信息保护认证制度，标志着我国进一步探索个人信息跨境的可行路径，为认证机构实施认证提供依据、亦为企业开展合规工作提供参考。如下要点值得特别关注。

其一，《认证规范》具有特定的适用范围。

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跨境处理活动。并且，《认证规范》要求处理者与境外接收方之间签订“具有法律约束力和执行力的文件”，并不限于“协议”，这与欧盟GDPR下的“有约束力的公司准则（BCRs）”或有相通之处，值得跨国公司关注。

2.受《个保法》域外管辖的境外处理活动。此时涉及颇具争议的一个问题——从境外直接收集个人信息是否适用《个保法》第三章的跨境规则。可能的解释包括：（1）从境外直接收集境内自然人的个人信息时，境外处理者即适用跨境规则，并由其在境内设置的专门机构或指定代表作为境内处理者；（2）个人信息出境后再次传输时，境外处理者才适用跨境规则，认证则是一种可行路径。

其二，《认证规范》数次强调监管响应与法律责任承担。

一方面，以境内实体作为我国监管的抓手：《认证规范》要求由跨国公司的境内公司、或境外处理者在境内的专门机构或指定代表申请认证，并由上述境内实体承担法律责任。该等法律责任带来的衍生效果包括，无关联关系的境内主体（如专业中介机构）对担任境外处理者的指定代表有较多顾虑，而没有境内关联实体的境外处理者在指定代表时可能面临困境。

另一方面，个人信息处理者和境外接收方均需承诺：遵守中国关于个人信息保护的法律与行政法规的保护标准，接受中国认证机构的监督（如答复询问、例行检查），并接受中国的司法管辖。

其三，《认证规范》重申、细化或提高了《个保法》关于个人信息跨境的合规要求。

《认证规范》的基本要求包括：个人信息处理者和境外接收方均应指定个人信息保护负责人（由决策层成员担任）和保护

机构，签订具有法律约束力和执行力的文件（“**法律文件**”），明确各方统一遵守的个人信息跨境处理规则（包括个人信息的类型与数量、处理目的与方式、存储期限、中转地、个人信息主体权益保障、安全事件处理等），并由处理者事先开展个人信息保护影响评估。

此外，《认证规范》特别强调对个人信息主体权益的保障，将《个保法》下的个人信息主体权利（包括提起诉讼）的行使扩展至境外接收方；同时，明确个人作为上述法律文件中涉及个人信息主体权益相关条款的受益人，有权要求获取该等条款的副本。该等要求与GDPR标准合同条款（“**SCCs**”）的思路亦有相通之处。

二、数据安全管理认证

2022年6月5日，国家市场监督管理总局与国家互联网信息办公室联合发布《关于开展数据安全管理认证工作的公告》（含《数据安全管理认证实施规则》），明确数据安全管理认证（“**DSM认证**”）工作的认证依据、认证模式与实施程序等。认证证书有效期为三年。

DSM认证是有资格的认证机构对组织（即认证委托人）的数据安全管理体系是否符合相关标准规范的评定活动，属于鼓励性活动。《网络安全法》《数据安全法》《个保法》均有认证相关规定，2019年发布的《数据安全管理办法（征求意见稿）》也明确鼓励网络运营者自愿通过数据安全管理认证。DSM认证扩充了现有数据安全认证机制，方便组织在开展“App安全认证”之外依据自身需求申请数据安全管理体系认证。

DSM认证的主要认证依据系《信息安全技术 网络数据处理安全要求》（GB/T 41479），主要包括数据处理安全总体要求（数据识别、分类分级、风险防控、审计追溯）、数据处理安全技术要求（包括收集、存储、使用、传输、删除和匿名化等）以及数据处理安全管理要求（数据安全责任人、人力资源保障及考核、事件应急处置）三个方面。该要求覆盖面广、颗粒度细，为组织数据合规提供明确指引，但也为认证工作开展提出核验难题。以第5.2（e）条关于从其他途径获取个人信息的合规要求为例，其提到组织需“了解个人信息来源、个人信息提供方已获得的个人信息处理授权同意范围”，对此认证时组织提供承诺函、相关合同条款即可，还是需要提供方实质证明数据来源的合法性，甚至要求组织采取必要核验措施？此有待进一步实践观察。

DSM认证的特点之一为将技术验证和现场审核作为认证的重要环节，此要求企业在制度文件体系以外，还需将数据管理工作落实到技术层面。实施流程包括认证委托、技术验证、现场审核、认证结果评价和批准、获证后监督共五步，其中技术验证环节会委托技术验证机构开展并参考其出具的技术验证报告进行评定。**中国网络安全审查技术与认证中心（“CCRC”）负责DSM认证的具体建设和实施工作，接受公众咨询和认证申请**。截至目前，CCRC已为DSM认证搭建公众联系专线及主题页面，且预设“数据安全管理认证申办系统”窗口，但系统窗口未正式启用，认证相关实施规则、申请书材料等尚未公布。此外，经了解，不排除未来CCRC委派其他认证机构承担DSM认证的可能性，有待持续关注。

*实习生陈瑞庭、张宜轩对本文亦有贡献