汉坤法律评述
2022 年 5 月 5 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 海口 | 香港

《网络安全标准 — 个人信息跨境处理活动认证技术规范（征求意见稿）》简评

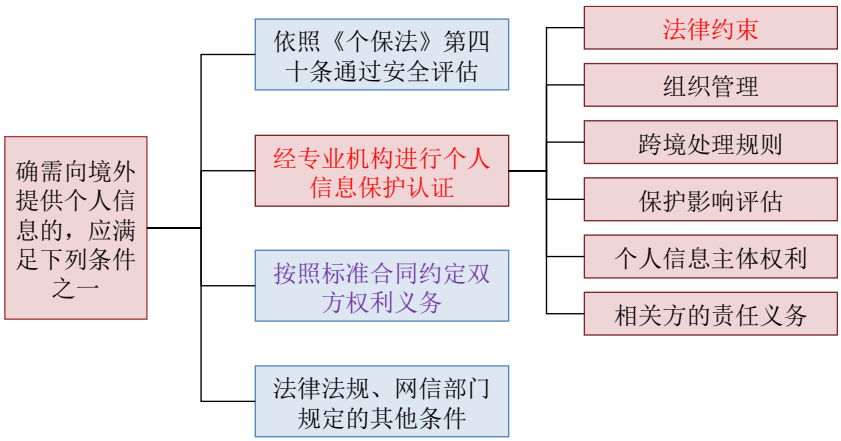
作者：段志超 | 蔡克蒙 | 胡敏喆[1]

2022 年 4 月 29 日，信息安全标准化技术委员会发布《网络安全标准 个人信息跨境处理活动认证技术规范（征求意见稿）》（“**《规范》征求意见稿**”），向社会公开征求意见。《规范》征求意见稿是首个对个人信息保护认证进行探索的官方文件，旨在落实《个人信息保护法》第三十八条第一款第二项提出的个人信息保护认证制度，便利个人信息跨境处理活动。我们将在下文梳理、总结《规范》征求意见稿中关于个人信息保护认证的关键要点，并同时作出我们的解读。

一、体系定位：个人信息出境机制之一

《个人信息保护法》第三十八条规定了在不触发个人信息出境政府评估的情况下的四种个人信息出境机制。《规范》征求意见稿则以“自愿认证”为基本原则，旨在落实《个人信息保护法》第三十八条第一款第二项提出的个人信息保护认证制度。

需要说明的是，根据《个人信息保护法》第四十条的规定，关键信息基础设施运营者或处理个人信息达到网信部门规定数量的个人信息处理者向境外提供个人信息依然应当通过国家网信部门组织的安全评估，认证无法替代政府安全评估要求。除此之外，在其他非强制要求评估的情况下，按照《规范》征求意见稿进行的个人信息保护认证可以作为数据出境的方式。



[1] 实习生金今对本文的写作亦有贡献。

二、认证适用的范围：跨国公司数据跨境传输以及境外个人信息处理者

《规范》征求意见稿适用于跨国公司或者同一经济实体、事业实体内部的个人信息跨境处理活动，以及《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，在境外处理境内自然人个人信息的活动。

就集团内部的个人信息跨境传输，《规范》征求意见稿的规定和欧盟的GDPR项下的“约束性公司规则”（Binding Corporate Rules，“**BCR**”）类似，集团内部的个人信息跨境处理活动可以由境内一方申请认证，并承担法律责任。具体而言，《规范》征求意见稿要求相关境外方指定个人信息保护负责人并在中华人民共和国境内设立专门机构，负责处理个人信息保护相关事务。参照相关实践，该等专门机构通常由集团内的境内关联方担任。

《规范》征求意见稿适用于《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还带来了一个问题，即《个人信息保护法》第三条第二款所规定的境外个人信息处理者直接收集境内个人信息是否属于《个人信息保护法》第三章所规定的个人信息跨境活动。一些业内人士参考 GDPR 的经验认为二者应是互斥关系，境外个人信息处理者直接收集境内个人信息并不属于第三章所规定的向境外提供个人信息，亦不适用相关规则，但《规范》征求意见稿的规定似乎否认了这种看法。

三、完成认证的主体：由境内主体完成认证

根据《规范》征求意见稿，应由下表所示境内主体完成认证，并承担法律责任：

适用情形	认证申请主体
跨国公司或者同一经济实体、事业实体内部的个人信息跨境处理活动	境内一方
《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，在境外处理境内自然人个人信息的活动	境外组织机构在境内设置的专门机构或者代表

《规范》征求意见稿仅要求处理者在境内的主体进行认证申请的规定似乎与国家网信办在 2021 年 11 月发布的《网络数据安全管理条例（征求意见稿）》所规定的“**数据处理者和数据接收方均**通过国家网信部门认定的专业机构进行的个人信息保护认证”有所差异。认证是否以及如何涵盖境外接收方仍有待法规或标准明确。

四、进行认证的机构：暂未明确

《个人信息保护法》仅规定应“按照国家网信部门的规定经过专业机构进行认证”。此次《规范》征求意见稿也暂未明晰进行认证的专业机构需满足的条件，但确定了认证机构有权对相关方做出的承诺进行监督。

五、法律约束：需签署具有约束力和执行力的文件

根据《规范》征求意见稿的要求，参与个人信息跨境处理的相关方之间需要签署具有法律约束力和执行力的文件，以确保个人信息主体权益得到充分保障，但该文件不一定是数据出境标准合同（实际上，《个人信息保护法》第三十八条将认证作为与数据出境标准合同并行的个人信息出境机制加以规定），也可能以数据处理协议或承诺函的形式进行签署。文件应当明确的重点内容如下：

- 参与个人信息跨境处理活动的相关方；
- 跨境处理个人信息的**目的**以及个人信息的**类别、范围**；
- 个人信息主体**权益保护措施**；
- 各相关方**承诺并遵守**统一的**个人信息处理规则**，并确保个人信息**保护水平不低于**中华人民共和国个人信息保护相关法律、行政法规规定的标准；
- 各相关方承诺接受认证机构监督；
- 各相关方**承诺接受**中华人民共和国个人信息保护相关法律、行政法规**管辖**；
- 明确在中华人民共和国**境内承担法律责任的组织机构**；
- 其他应当遵守的法律、行政法规规定的义务。

六、完成认证需要遵守的条件：多维度全面规定

除法律约束外，《规范》征求意见稿还从组织管理、跨境处理规则、个人信息保护影响评估、个人信息主体权益保障等维度全方位地对认证条件进行了规定，详见下表：

认证要求	要点
组织管理	**个人信息保护负责人：** ■ 相关方均应指定； ■ 具备个人信息保护专业知识和相关工作经历； ■ 由本组织机构决策层成员承担； ■ 应为个人信息保护工作承担下列职责： 1. 明确主要目标、基本要求、工作任务、保护措施； 2. 提供人力、财力、物力保障，确保所需资源可用； 3. 指导、支持相关工作人员开展工作，确保达到预期目标； 4. 向主要负责人汇报工作情况，推动持续改进。
	个人信息保护机构： ■ 相关方均应设立； ■ 履行个人信息保护义务； ■ 防止未经授权的访问、个人信息泄露、篡改、丢失； ■ 应在个人信息跨境处理活动中承担下列职责： 1. 制定实施各相关方均认可的活动计划； 2. 组织开展个人信息保护影响评估； 3. 监督本组织机构按照约定的规则处理跨境个人信息； 4. 接受处理个人信息主体的请求和投诉。

认证要求	要点
跨境处理规则	参与个人信息处理的相关方遵守统一的个人信息跨境处理规则，至少包括下列事项：跨境处理个人信息的基本情况，包括个人信息类型、敏感程度、数量等；跨境处理个人信息的目的、方式和范围；个人信息境外存储的起止时间及到期后的处理方式；跨境处理个人信息需要中转的国家或者地区；保障个人信息主体权益所需资源和采取的措施；个人信息安全事件的赔偿、处置规则。
个人信息保护影响评估	参照《个人信息保护法》及《信息安全技术 个人信息安全影响评估指南（GB/T 39335-2020）》进行。
个人信息主体权益保障	■ 遵守《个人信息保护法》规定，保障信息主体的各项权利，包括知情权、决定权、对其个人信息进行查阅、复制、更正、删除的权利、拒绝自动化决策的权利等。 ■ 当出现难以保证跨境个人信息安全的情况时，应当及时终止跨境处理个人信息； ■ 境内法律负责承担方承诺为个人信息主体行使权利提供便利条件，并承担损害赔偿责任； ■ 承诺接受中国认证机构的监管； ■ 承诺遵守中国法律法规，接受中国法律管辖。

七、小结

从征求意见稿的具体内容来看，《规范》征求意见稿参考了 GDPR 规定的“约束性公司规则”和“行为准则”（Code of Conduct），旨在为集团内部多方主体间跨境传输个人信息提供便利以及兼顾为境外主体在境外处理境内自然人个人信息的活动提供合规路径。由于《规范》征求意见稿规定的要求仅供认证机构在开展认证时进行判断，并未像 GDPR 一样要求约束性公司规则或行为准则需经数据保护主管机关的批准，因此我国的认证机制未来在实践层面可能更具灵活性。目前《规范》征求意见稿主要针对实体标准进行了较为细致的规定，我们期待《规范》征求意见稿或其他法规、标准后续可以进一步明确认证机构、认证流程等事项，以为制度的落地提供更明确的指引。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

蔡克蒙

电话： +86 10 8516 4289
Email： kemeng.cai@hankunlaw.com