跨境认证——解读个人信息出境的第三条路

作者：杨建媛 邬丹 李天烁

引言

2022 年 11 月 18 日，国家互联网信息办公室（“**网信办**”）公开发布了《关于实施个人信息保护认证的公告》及其附件《个人信息保护认证实施规则》，规定了开展个人信息保护认证（区分两种情形：不含跨境处理活动、包含跨境处理活动，后者简称“**跨境认证**”）的程序性规则。个人信息保护认证的认证依据为推荐性国家标准 GB/T 35273《信息安全技术 个人信息安全规范》；涉及跨境处理活动时，认证依据还包括全国信息安全标准化技术委员会（“**信安标委**”）发布的标准相关技术文件 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》（均执行最新版本）。

2022 年 11 月 8 日，信安标委发布了《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 V2.0（征求意见稿）》（“**《跨境认证规范 V2.0》**”或“**V2.0**”），此时距离其于 2022 年 6 月 24 日发布第一版（“**《跨境认证规范 V1.0》**”或“**V1.0**”）仅过去了四个多月。

跨境认证是《个人信息保护法》（“**《个保法》**”）第 38 条第 1 款规定的跨境机制之一。个人信息处理者向境外提供（又称“**跨境传输**”、“**出境**”）个人信息，应择一满足安全评估（如适用，需优先满足）、跨境认证、标准合同、或其他条件。

其一，安全评估具有优先地位和国家安全站位，如果落入安全评估的适用范围，则必须向网信办申报安全评估。其二，跨境认证由专业机构对个人信息处理者及境外接收方的数据保护水平进行审查，不仅可以作为跨境机制，亦可成为企业证明自身合规水平的有效方式。其三，标准合同是一种无需审查、相对轻量级的跨境机制，企业可以充分利用网信办发布的标准合同模板，通过境内外双方自主缔约的方式，高效便捷地开展个人信息出境活动。其四，我国立法、执法机构尚未正式规定个人信息出境的其他条件，有待后续观察。

上述跨境机制的配套实施规则正在陆续出台。网信办现已发布《数据出境安全评估办法》《个人信息出境标准合同规定（征求意见稿）》，相应的解读文章请参阅《*海问 •观察丨数据流动的分寸：评析〈数据出境安全评估办法〉*》《*海问 •观察丨透视“中国版 SCC”——个人信息出境标准合同*》。

本文将具体结合《跨境认证规范 V2.0》对跨境认证制度进行重点解读，以期为企业提前研判跨境认证提供参考。

一、 跨境认证的制度逻辑：侧重考察处理者的个人信息保护“能力”

作为个人信息跨境的前提条件，安全评估、标准合同、认证这三项机制具有内在共性：形式上，均要求个人信息处理者事前自行开展评估、并与境外接收方签署具有法律约束力的协议或文件；实质上，均强调境外接收方的同等保护水平、

以及个人信息主体的权益保护。

与此同时，不同的跨境机制也存在制度逻辑的差异。安全评估不限于个人层面的保护，兼具国家安全的宏观站位；安全评估、标准合同更侧重于以数据出境场景为对象进行个案分析，而认证兼具以个人信息处理者、境外接收方为对象进行个体分析，当其数据保护能力达到我国法的要求，则个人信息可在认证范围内进行传输。认证或可在一定程度上超脱一事一议的局限性、彰显企业本身的数据保护能力，因此，认证不仅能单独作为跨境传输的合规机制，也能成为企业向监管机构、合作方、用户展示其合规水平的有力证明。

此外，跨境认证作为一套体系化的合规安排，往往需要更多的资源投入，例如《跨境认证规范 V2.0》关于个人信息跨境处理规则、组织管理机构的额外规定。因此，跨境认证往往适用于合规建设较为完善、境内外双方或多方关系较为密切或合作长期稳定的情形，例如跨国集团内部的个人信息跨境传输。

二、 跨境认证的适用范围：包括但不限于“集团内跨境”、“域外管辖”

《跨境认证规范 V1.0》曾将跨境认证的适用范围限于两种特殊情形：其一，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（“**集团内跨境**”）；其二，《个保法》第 3 条第 2 款适用的个人信息处理活动（“**域外管辖**”）。

《跨境认证规范 V2.0》则将跨境认证的适用范围扩张至“个人信息处理者开展个人信息跨境处理活动”，恢复了跨境认证的通用性。但 V2.0 仍在第 2 条“认证主体”中特别列举了集团内跨境、域外管辖这两种情形，这既点出了跨境认证的典型适用场景，也解答了业界的一个困惑——从境外直接收集境内个人信息是否适用《个保法》第三章的跨境规则。目前看来，境外处理者仍需就个人信息跨境处理提前做好合规准备，并在必要时与监管部门沟通确认。

三、 跨境认证的双方性：个人信息处理者、境外接收方均需进行认证

《跨境认证规范 V2.0》在全文多处强调认证的双方性，个人信息处理者（即境内提供方）、境外接收方双方均需遵守关于基本原则、具有法律约束力的文件、组织管理要求、个人信息跨境处理规则、个人信息主体权益保障等方面的要求。实际上，跨境认证覆盖了“境内处理—跨境传输—境外处理”的个人信息跨境处理活动全流程。根据《个人信息保护认证实施规则》，认证程序中包括“技术验证”与“现场审核”，该等要求如何适用于境外接收方有待观察。

在欧盟《通用数据保护条例》（“**GDPR**”）项下，根据欧盟数据保护委员会（“**EDPB**”）于 2022 年 6 月最新发布的《关于认证作为传输工具的指南（公开征求意见稿）》，作为跨境传输工具的认证仅针对境外接收方这一方，且一般仅涵盖境外处理活动这一环节，而境内提供方的境内处理活动和跨境传输活动则直接适用 GDPR。

相较而言，我国的跨境认证不仅是对个人信息境外处理活动、境外接收方的考察，也包括对境内提供方的个人信息处理活动的全面考察。在《个保法》之外，《个人信息保护认证实施规则》《跨境认证规范 V2.0》均要求个人信息处理者同时符合推荐性国家标准 GB/T 35273《信息安全技术 个人信息安全规范》的要求。这进一步提升了企业获得跨境认证的难度和合规成本，但也相应提升了跨境认证

作为企业合规证明的含金量。

四、 跨境合规的内在共性：三大机制相互借鉴、部分融合

在《跨境认证规范》V1.0、V2.0 两个版本发布之间，网信办陆续发布了《个人信息出境标准合同规定（征求意见稿）》《数据出境安全评估办法》《数据出境安全评估申报指南（第一版）》，对标准合同、安全评估这两项跨境机制进行了细化规定。《跨境认证规范 V2.0》借鉴、融合了上述新规（尤其是标准合同）在法律文件、个人信息保护影响评估等方面的要求。

1. **具有法律约束力的文件**（“**法律文件**”）：关于法律文件的内容，V2.0 对 V1.0 的新增要求与标准合同有较高重合度（具体对比如下表），因此，企业在起草法律文件时可参考标准合同的相关条款。

《跨境认证规范 V1.0》	《跨境认证规范 V2.0》	《个人信息出境标准合同规定（征求意见稿）》	《数据出境安全评估办法》
图例： ~~删除~~ 调整 新增 其他法规相似条款			
4.1 有法律约束力的协议……文件应当至少明确下列内容：	5.1 具有法律约束力的协议……文件应至少明确下列内容：	第六条 标准合同包括以下主要内容：	第九条 ……法律文件中……至少包括以下内容：
a) ~~开展个人信息跨境处理活动的~~个人信息处理者和境外接收方	a) 个人信息处理者和境外接收方的基本信息，包括但不限于名称、地址、联系人姓名、联系方式等	（一）个人信息处理者和境外接收方的基本信息，包括但不限于名称、地址、联系人姓名、联系方式等	/
b) 跨境处理个人信息的目的~~以及个人信息的~~类别、范围	b) 个人信息跨境处理的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点等	（二）个人信息出境的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点等	（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等 （二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施
/	c) 个人信息处理者和境外接收方保护个人信息的责任与义务，以及为防范个人信息跨境处理可能带来安全风险所采取的技术和管理措施等	（三）个人信息处理者和境外接收方保护个人信息的责任与义务，以及为防范个人信息出境可能带来安全风险所采取的技术和管理措施等	/
c) 个人信息主体权益保护措施	d) 个人信息主体的权利，以及保障个人信息主体权利的途径和方式	（五）个人信息主体的权利，以及保障个人信息主体权利的途径和方式	（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等

			风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式
/	e) 救济、合同解除、违约责任、争议解决等	（六）救济、合同解除、违约责任、争议解决等	（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式
d) 境外接收方承诺并遵守统一的个人信息跨境处理规则，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	f) 境外接收方承诺并遵守同一个人信息跨境处理规则，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	/	/
e) 境外接收方承诺接受认证机构监督	g) 境外接收方承诺接受认证机构监督	/	/
f) 境外接收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	h) 境外接收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	/	/
g) 明确在中华人民共和国境内承担法律责任的组织	i) 明确在中华人民共和国境内承担法律责任的组织，并承诺履行个人信息保护义务	/	/
/	j) 个人信息处理者和境外接收方均承诺对侵害个人信息权益行为承担法律责任，法律责任不明确的，由个人信息处理者承担法律责任	/	/
h) 其他应当遵守的法律、行政法规规定的义务	k) 其他应遵守的法律、行政法规规定的义务	/	/

2. **个人信息保护影响评估/数据出境风险自评估**（合称“**自评估**”）：关于自评估的内容，V2.0 对 V1.0 的新增要求与标准合同有较高重合度（具体对比如下表），企业可在构建自评估框架时整合跨境认证和标准合同的报告模板。

《跨境认证规范 V1.0》	《跨境认证规范 V2.0》	《个人信息出境标准合同规定（征求意见稿）》	《数据出境安全评估办法》

图例：	~~删除~~	调整	新增	其他法规相似条款
4.4 个人信息保护影响评估 开展个人信息跨境活动的个人信息处理者事前评估向境外提供个人信息活动是否合法、正当、必要，所采取的保护措施是否与风险程度相适应并有效等，个人信息保护影响评估至少包括下列事项：	5.4 个人信息保护影响评估……评估报告应至少包括下列事项：	第五条 个人信息处理者向境外提供个人信息前，应当事前开展个人信息保护影响评估，重点评估以下内容：	第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：
a) 向境外提供个人信息是否符合法律、行政法规	a) 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	（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	（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性
b) 对个人信息主体权益产生的影响……	b) 跨境处理个人信息的规模、范围、类型、敏感程度、频率，个人信息跨境处理可能对个人信息权益带来的风险	（二）出境个人信息的数量、范围、类型、敏感程度，个人信息出境可能对个人信息权益带来的风险	（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险
/	c) 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障跨境处理个人信息的安全	（三）境外接收方承诺承担的责任义务，以及履行责任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	（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全
/	d) 个人信息跨境处理后泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等	（四）个人信息出境后泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等	（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等
b) ……特别是境外国家和地区的法律环境、网络安全环境等对个人信息主体权益的影响	e) 境外接收方所在国家或者地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响，包括但不限于：……	（五）境外接收方所在国家或者地区的个人信息保护政策法规对标准合同履行的影响	（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务
c) 其他~~维护个人信息权益所必需~~的事项	f) 其他可能影响个人信息跨境处理安全的事项	（六）其他可能影响个人信息出境安全的事项	（六）其他可能影响数据出境安全的事项

五、 跨境合规的路径选择：企业如何提前研判跨境认证

面对安全评估、标准合同、认证这三项跨境机制，建议企业提前就个人信息出境事宜进行整体布局，充分利用一项或多项跨境机制，以实现既高效、又合规的个人信息跨境流动。其一，安全评估具有优先地位，企业一旦落入安全评估的适用范围，则必须向网信办申报安全评估；其二，标准合同既可以单独作为跨境机制，其模板条款也可为安全评估、跨境认证中的法律文件提供参考；其三，跨境认证既可以单独作为跨境机制，也可成为企业数据保护水平的有力证明，与安全评估、标准合同并行不悖。

根据《个人信息保护认证实施规则》，认证证书有效期为 3 年。企业首次认证时，需要经过技术验证机构的“技术验证”、以及认证机构的“现场审核”。在认证证书的有效期内，通过认证机构的“获证后监督”保持其有效性；企业可在有效期届满前 6 个月内提出认证委托，由认证机构采用“获证后监督”的方式对符合认证要求的委托换发新证书。

跨境认证是一套体系化的合规安排，这也意味着较高的资源投入。建议企业充分考虑自身数据合规建设的现状或计划、以及企业和境外接收方的关系与合作，从而合理决策是否申请跨境认证。概括而言，《跨境认证规范 V2.0》主要包括以下方面的要求，值得企业重点考量：

1. **境外接收方**：V2.0 对境外接收方的同等保护水平提出了全方位的具体要求，并强调境外接收方在中国法下承担责任，且企业作为境内提供者可能为境外接收方承担“兜底责任”。

2. **组织管理要求**：V2.0 要求个人信息处理者、境外接收方均指定个人信息保护负责人、设立个人信息保护机构，并规定了具体的工作职责。

3. **个人信息跨境处理规则**：V2.0 要求个人信息处理者、境外接收方均遵守同一个人信息跨境处理规则，这似乎是区别于法律文件的另一套专门规则。

4. **法律文件**：V2.0 要求双方签署具有法律约束力和可执行的文件或协议，安全评估、标准合同也有类似要求，且 V2.0 对法律文件内容的规定与标准合同高度重合。

5. **自评估**：V2.0 要求个人信息处理者事先自行开展个人信息保护影响评估，安全评估、标准合同也有类似要求，且 V2.0 对评估内容的规定与标准合同高度重合。

6. **个人信息主体权益保障**：V2.0 要求个人信息处理者、境外接收方共同保障个人信息主体的权益，且该等具体规定较多借鉴了标准合同的相关条款。