# 数据合规透视

作者：杨建媛

## 中国关于个人信息跨境传输机制的最新进展

根据《个人信息保护法》（“**《个保法》**”）第38条，个人信息处理者向中华人民共和国境外（“**中国**”，仅为本文之目的，不含香港特别行政区、澳门特别行政区和台湾省）提供个人信息，应当具备下列条件之一：通过国家网信部门组织的安全评估、经专业机构进行个人信息保护认证、与境外接收方订立标准合同、或满足其他法定条件。

为落实《个保法》下的个人信息跨境传输机制，我国已于2021年10月发布了《数据出境安全评估办法（征求意见稿）》，并于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》《个人信息出境标准合同规定（征求意见稿）》及《个人信息出境标准合同（征求意见稿）》。

### 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《个人信息出境标准合同（征求意见稿）》的思路亦有相通之处。

## 二、个人信息出境标准合同

2022年6月30日，国家互联网信息办公室发布了《个人信息出境标准合同规定（征求意见稿）》（“**《规定》**”）及《个人信息出境标准合同（征求意见稿）》（“**《标准合同》**”），为《个保法》下个人信息跨境条件之一的“标准合同”提供了落地方案。

《标准合同》在相当程度上借鉴了欧盟标准合同条款（“**SCC**”），同时体现了我国个人信息保护与监管的特色与侧重点。海问律师已协助众多中国企业落地欧盟SCC，特别是Schrems II案后应对额外的实质保障与补充措施要求。企业可以参考《规定》及《标准合同》所体现的最新趋势，提前开展个人信息跨境提供的合规部署工作，并对基于欧盟GDPR的跨境框架（如有）进行相应的调整。其中，如下要点值得特别关注。

### 1.厘定标准合同的适用范围，大量出境个人信息的企业或难适用标准合同

根据《规定》，适用标准合同的个人信息处理者（“**处理者**”或“**境内提供方**”）需同时符合以下情形：（1）非关键信息基础设施运营者，（2）处理个人信息不满100万人，（3）自上年1月1日起累计向境外提供未达到10万人个人信息，且（4）自上年1月1日起累计向境外提供未达到1万人敏感个人信息。

与上述任一情形相反，即为《数据出境安全评估办法（征求意见稿）》（“**《评估办法》**”）的适用范围，需通过网信部门进行安全评估。但《规定》就出境累计计算新增了“自上年1月1日起”的限定，即累计期间最多不超过2年，适当放松了对出境活动的监管。不过，基于我国的人口基数，上述100万、10万、1万的门槛实际较低，并且以处理者整体为单位，并不区分业务场景，因此，实践中大量企业可能无法适用标准合同，而需进行安全评估。

此外，标准合同与安全评估在实践中仍有相通之处。例如，《评估办法》要求处理者与境外接收方拟订合同等具有法律效力的文件，且对合同内容的要求与《标准合同》存在大量重合之处。《标准合同》由国家网信部门制定，企业即使不直接适用标准合同，也可以参考《标准合同》来拟定数据出境相关合同。

### 2.标准合同要求备案，为事后监管提供抓手

《规定》对标准合同采用“自主缔约与备案管理相结合”的监管路径。一方面，标准合同无需事前审批即可生效。另一方面，境内提供方应在标准合同生效之日起10个工作日内，向所在地省级网信部门备案，备案时应提交标准合同（除格式条款外，还包含个案具体的保护措施及出境情况说明）、个人信息保护影响评估报告。

对比欧盟GDPR，在Schrems II案后，欧盟固然对SCC提出了更高的要求——境内提供方需证明个人数据出境后实质上可达到欧盟同等保护水平，而非仅是形式上签署SCC文本，但仍不要求备案SCC。

《规定》要求备案标准合同，虽然区别于安全评估的个案事前审批，但给监管留足了事后审查的抓手——省级以上网信部门发现个人信息出境活动不再符合监管要求，则书面通知处理者终止出境活动。处理者违反备案要求的，责令限期改正；

拒不改正或损害个人信息权益的，责令停止个人信息出境活动，依法予以处罚；构成犯罪的，依法追究刑事责任。

### 3.细化出境场景下的个人信息保护影响评估，且评估报告要求备案

《个保法》提出了个人信息保护影响评估（“**PIA**”），并规定了各个适用场景通用的评估项：（1）处理目的、处理方式等是否合法、正当、必要，（2）对个人权益的影响及安全风险，（3）保护措施是否合法、有效并与风险程度相适应。

《规定》针对出境场景，进一步细化了PIA的评估项，额外强调了：（1）境外接收方对履行个人信息保护义务与责任的承诺、措施、能力，（2）个人信息出境后被泄露、损毁、篡改、滥用等风险，（3）境外接收方所在国家或地区（“**境外接收地**”）的个人信息保护政策法规对履行标准合同的影响。《规定》要求处理者备案PIA报告，但并未具体规定报告的颗粒度，这可能成为企业合规实践的关注重点之一。

《规定》的PIA与《评估办法》的数据出境风险自评估的评估项多有相似，不同之处在于，后者额外强调评估数据出境对国家安全、公共利益、个人或组织合法权益的风险，或许是安全评估还涉及重要数据、大量数据的特殊性质使然。

### 4.中国版TIA：评估境外接收地的个人信息保护政策法规对履行标准合同的影响

《规定》要求处理者在PIA中评估境外接收地的个人信息保护政策法规对履行标准合同的影响，并在《标准合同》第4条规定了评估的具体内容。究其渊源，欧盟在Schrems II案中对SCC这一跨境工具进行加码，额外要求对数据接收地的法律及实践是否妨碍数据接收方履行合同义务进行评估（“**传输影响评估/TIA**”），TIA亦成为最新版SCC的组成部分。

中国版TIA已在欧盟的基础上进行了简化，但于企业而言仍属于高难度的合规动作，我们结合基于GDPR的跨境框架开展TIA的实践经验，提示在我国《标准合同》下开展TIA的核心考虑点如下。

| 维度 | 《标准合同》规定 | 实践困惑 |
| --- | --- | --- |
| 形式要件 | **义务主体**：TIA 主要为境内提供方的义务，但境外接收方有义务尽最大努力提供必要信息、及时通知相应变化，且双方均应就 TIA 进行保证、声明与记录。 | **境内主体开展域外法评估。**因涉及域外法，境内提供方在进行评估时，如何证明其评估基础准确、充分、实时，如何证明已尽到“合理努力”，如何协调境外接收方甚至境外律师。 |
| | **评估标准**：“经过合理努力”仍“不知晓”境外接收地的个人信息保护政策法规会阻止境外接收方履约。 | |
| 实质要件 | **评估对象**：境外接收地的个人信息保护政策法规对遵守“本合同”条款的影响，是否会阻止境外接收方履行“本合同”规定的义务。 | **个案评估亦或宏观评估。**根据文意，系以特定个人信息跨境传输、特定数据接收方为单位进行个案评估，而非以境外接收地为单位进行宏观评估。 |
| | **评估依据**：境外接收地与个人信息保护相关的法律法规与标准、国际组织与国际承诺、监督执法机构与司法机构，尤其强调境外公共机关要求境外接收方提供或访问个人信息的法规要求和历史经验。 | **仅为法律法规评估还是也包括执法实践评估。**根据文意，主要是个人信息保护相关的法律法规评估，有限的执法实践评估仅针对境外接收方自身。 |

### 5.采取合适的技术、管理措施，切实保障个人信息安全

标准合同并不限于单纯的文本，其中约定的技术、管理措施是降低个人信息出境安全风险更为直接、有效的方式，也是合同履行与合规实践中的重难点。《标准合同》要求由缔约方自行列明所采取的技术、管理措施，并提供加密、匿名化、去标识化、访问控制作为示例。欧盟在SCC附录二、EDPB关于补充措施的指南中对该等措施进行了详细的提示，在实践中可供企业参考。

安全并非绝对的概念，《标准合同》也对技术、管理措施进行了限定：一方面，境内提供方需尽“合理的”努力确保境外接收方采取安全措施，且安全措施系综合考虑个人信息出境的具体事实进行个案选择。另一方面，境外接收方需采取“有效的”措施，并定期检查以维持“适当的”安全水平。实践中，安全措施的把握尺度必将成为重点课题，也不太可能有标准答案。

**6.具体规制个人信息出境后的二次传输，以书面协议保障同等保护水平**

《个保法》对处理者“向境外提供”个人信息进行了规制，而除了个人信息从我国境内到境外的“一次传输”，《评估办法》已注意到了数据出境后的“再转移”问题，《标准合同》则在境外接收方的义务中规制个人信息的“再提供”（即“**二次传输**”）。

根据《标准合同》，境外接收方不得将个人信息提供给位于中国境外的第三方，除非同时符合以下要求：（1）确有业务需要；（2）已告知个人，并取得单独同意（除非法律法规另有规定）；（3）与第三方达成书面协议，确保第三方达到同等保护水平，并承担连带责任；（4）向境内提供方提供与第三方的协议副本。并且，《标准合同》附录一要求说明该等第三方。

我国试图通过境外接收方的合同义务，在二次传输环节延展我国的个人信息保护标准，但实践中可能存在以下难点：（1）在签订标准合同时，境外接收方难以准确预估二次传输的需求，尤其是第三方的具体身份（欧盟SCC则允许仅向个人告知第三方的类型）；（2）《标准合同》并未指明“单独”同意的颗粒度；（3）二次传输要求签订协议，但并未指明可否适用《个保法》第38条的其他条件（欧盟SCC则允许二次传输使用GDPR下的多项跨境传输工具）。

**7.扩张审计的适用，境外接收方有义务就合同项下的处理活动接受审计**

在个人信息保护的语境下，“审计”是相对较新的概念，也是比较强势的合规监督措施。《个保法》提出了处理者针对自身处理活动的合规审计，国家标准《信息安全技术 个人信息安全规范》（GB/T 35273-2020）提出了处理者对于受托方、第三方接入工具（如SDK）的审计。

《标准合同》进一步扩张了审计的应用场景，可能成为双方签约的谈判难点。境外接收方无论是独立的处理者还是委托处理的受托方，均有义务允许并配合境内提供方对本合同涵盖的处理活动进行审计，且境内提供方有义务根据相关法律法规要求向我国监管机构提供该等审计结果。对比欧盟SCC，仅受托方有义务允许该等审计，两个独立的处理者之间并不要求审计，除非监管机构要求对境外接收方进行审计。

此外，《标准合同》规定了境外接收方需向境内提供方提供审计报告的两种情形：（1）合同解除时，对个人信息进行销毁或匿名化处理；（2）作为受托方，在超出存储期限后，对个人信息进行删除或匿名化处理。在类似情形下，欧盟SCC仅要求境外接收方进行“证明（certify）”，而《标准合同》进一步要求“提供审计报告”，这也体现了监管机构对于审计这一形式的认可。

**8.个人有权要求双方提供具体的合同副本，进一步落实知情权**

《个保法》明确了个人的知情权，并要求处理者公开个人信息处理规则。《标准合同》则进一步提出，境内提供方、境外接收方均有义务经个人要求而提供标准合同副本。欧盟SCC也有类似要求，据观察实践中尚未得到充分落实。

合同副本不限于网信办制定的格式条款，也包括标准合同中针对个案具体的保护措施及出境情况说明，这是保障个人对其个人信息处理活动的知情权的应有之义。同时，《标准合同》也考虑到了企业保护商业秘密或其他机密信息的需求，允许对合同副本进行适当遮蔽，但仍需向个人提供有效摘要以助其理解合同内容。

企业在拟定标准合同时可以就此提前筹划：一方面，合理设计标准合同副本，平衡个人知情权与企业机密保护；另一方

面，合理设计个人身份及其个人信息所涉出境活动的确认机制，有针对性地提供副本，避免企业标准合同的大规模流通。