个人信息出境机制全面落地：标准合同的规则与文本

作者：杨建媛 邬丹

2023年2月22日，国家互联网信息办公室（“网信办”）发布《个人信息出境标准合同办法》（“《标准合同办法》”）及其附件《个人信息出境标准合同》（“《标准合同》”）。《标准合同办法》将于2023年6月1日起施行，并对此前已开展的个人信息出境活动予以6个月的整改宽限期，即应在2023年12月1日之前完成整改。

至此，随着《数据出境安全评估办法》《关于实施个人信息保护认证的公告》《个人信息跨境处理活动安全认证规范》《标准合同办法》的相继出台与施行，我国《个人信息保护法》关于个人信息出境的三大合规机制——安全评估、认证、标准合同进入落地阶段。**三种出境机制均涉及数据盘点、自评估、法律文件签署等前期工作，需要预留充分的准备时间，企业已经来到了出境合规的关键时点。**

本文将分为上下两篇，上篇重点解读适用《标准合同办法》的核心关注点、下篇预测《标准合同》谈判签署中可能的疑难条款，为企业使用标准合同实现个人信息出境合规提供参考。关于安全评估、认证的解读，请见往期文章《数据流动的分寸：评析〈数据出境安全评估办法〉》和《跨境认证——解读个人信息出境的第三条路》。

上篇：作为出境机制的标准合同

《标准合同办法》明确了标准合同作为一种个人信息出境机制的适用门槛、备案要求、条款内容、自评估要求等内容，为标准合同的落地实施奠定了基础。

一、适用门槛与安全评估泾渭分明

标准合同与安全评估的适用条件相对立（详见下表）。**企业如果未达到安全评估的申报门槛，才可以选择标准合同作为个人信息出境的合规机制。**

标准合同的适用条件	安全评估的适用条件
1. **非**关键信息基础设施运营者；	1. **关键信息基础设施运营者**；
2. 处理个人信息**不满**100万人；	2. 处理**100万人**以上个人信息；
3. 自上年1月1日起累计向境外提供个人信息**不满**10万人；**且**	3. 自上年1月1日起累计向境外提供**10万人**个人信息；**或**
4. 自上年1月1日起累计向境外提供敏感个人信息**不满**1万人。	4. 自上年1月1日起累计向境外提供**1万人**敏感个人信息。
法律、行政法规或者国家网信部门另有规定的，从其规定。	国家网信部门规定的其他需要申报数据出境安全评估的情形。

此外，《标准合同办法》中特别强调企业**不得采取数量拆分等手段，规避安全评估的适用**。根据我们的实践经验，数量拆分可能包括如下情形：（1）将个人信息拆分至**不同的公司实体**，从而降低每个实体所处理或出境的个人信息数量；（2）将个人信息拆分至**不同的时间周期**，从而降低特定区间所涉的个人信息数量。

在实践中，大型集团公司的组织架构与IT架构比较复杂，可能存在多个公司实体、多条业务线共用信息系统、个人信息的情形。对此，企业在进行数据盘点时需要区分符合实际情况的“**客观型拆分**”、为了绕开安全评估的“**规避型拆分**”，可以考虑以下因素：（1）**处理目的**：企业是否需要在业务中使用个人信息；（2）**数据控制力**：企业是否分别控制不同的服务器、信息系统（物理隔离），或者在同一信息系统中具有清晰的权限区分（逻辑隔离）。

二、备案要求与合同缔结既分立又关联

《标准合同办法》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（对比：安全评估为事前审批），标准合同生效后可开展个人信息出境活动。另一方面，企业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**，提交（1）标准合同、（2）个人信息保护影响评估（“**自评估**”或“PIA”）报告。

标准合同的备案为网信部门的事后监管提供了抓手——省级以上网信部门发现个人信息出境活动存在较大风险或者发生个人信息安全事件的，可以依法对个人信息处理者进行约谈；个人信息处理者应当按照要求整改，消除隐患。

相较于通过安全评估的结果有效期为2年，**标准合同并没有期限规定**，企业可以在标准合同中自主约定合同的有效期。**但签订标准合同并备案也并非一劳永逸**，如果发生以下情形，企

业应重新开展自评估、补充或重订标准合同、并履行备案手续。

（1）**事实情况变化**：向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的。

请注意，从《标准合同办法》字面来看，出境个人信息“规模/数量”发生变化不在此列；但另一方面，如果出境数量到达10万人个人信息或1万人敏感个人信息（自上年1月1日起算），则将适用安全评估。

（2）**境外接收地法律变化**：境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等，可能影响个人信息权益的。

请注意，只有政策法规变化且可能影响个人信息权益的方在此列。

（3）**其他**：可能影响个人信息权益的其他情形。

三、标准合同带来的便捷与挑战

标准合同应当严格按照网信办制定的《标准合同》订立，不能修改既定的模板与条款。与此同时，**《标准合同》也给双方留出了一定的灵活空间**，设置了附录二“双方约定的其他条款（如需要）”，但不得与标准合同相冲突。与之类似，欧盟标准合同条款（SCC）也允许合同双方在标准合同条款之外增加额外条款，只要该等条款不与既有条款相冲突、也不损害个人的基本权利与自由。

根据我们的实践经验，境外接收方在履行《标准合同》个别既定条款时可能面临挑战。关于《标准合同》疑难条款的解读，请见本文《下篇：作为协议条款的标准合同》。

四、自评估要求使标准合同趋同于其他出境机制

1. 个人信息保护影响评估/PIA

《个人信息保护法》要求对影响较大的个人信息处理活动（包括但不限于出境）开展个人信息保护影响评估（“**自评估**”或“**PIA**”），并规定了自评估的通用内容：（1）个人信息的处理目的、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）所

采取的保护措施是否合法、有效并与风险程度相适应。

针对个人信息出境，关于安全评估、标准合同、认证的配套法规均在《个人信息保护法》的基础上扩展了自评估的内容，且**自评估的内容具有较高重合度**（详见下表），有需要的企业或可在设计自评估模板时进行通盘考虑。

、

为开展自评估，企业需要对以下情况进行盘点与分析：

（1）**数据出境的基础事实**：包括个人信息的种类、数量、敏感程度，处理的目的、方式，境外接收方的范围等；

（2）**数据出境的合规性**：包括个人信息出境的合法性（如告知个人、满足合法性基础等），正当性（如目的正当、手段正当、过程正当），必要性（如数据类型、数量级、保存期限的最小必要）；

（3）**数据出境的风险**：包括正常情况下数据出境本身对于个人信息权益的风险，以及发生数据安全事件的风险、对个人权益的影响及维权渠道；

（4）**境外接收方的情况**：包括境外接收方关于个人信息的管理措施、技术措施、保护水平（即硬实力），以及境外接收方通过《标准合同》等法律文件承担的数据安全与保护义务（即约束力）；

（5）**境外接受地的法治情况**：包括境外接收地关于个人信息保护的立法与监管情况，是否会影响境外接收方履行本《标准合同》。详见“四、2. 传输影响评估/TIA”。

2. 传输影响评估/TIA

欧盟在Schrems II案中对标准合同条款（SCC）这一跨境工具进行加码，额外要求对境外接收地的法律及实践（尤其是政府机构调取数据的权力）是否妨碍境外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。

究其根源，即便合同对境外接收方施加了约束、且境外接收方真诚地愿意履行合同义务，但如果境外接受地的法治环境发生重大变化，境外接收方仍可能因为国家监管层面的“不可抗力”而无法履行合同义务，从而无法保障数据安全。

我国《标准合同》第四条也专门规定了“境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响”，包括如下两个层面。**中国版TIA结合了宏观评估与个案评估，对于整体法治环境一般的境外接受地，也可能因个案情况不敏感、境外接收方的相关记录良好而得出比较乐观的评估结论。**

（1）**针对境外接受地的宏观评估**：TIA应当评估境外接受地关于个人信息保护的立法与标准、国际组织与国际承诺、执法及司法机构。但从字面上看，并不包含对于法律实践情况的整体评估。

（2）**针对特定数据出境活动的个案评估**：TIA应当结合本《标准合同》项下数据出境活动的事实情况，以及该特定境外接收方的数据保护能力、关于数据安全事件、政府数据调取的负面历史。

对比此前的征求意见稿，《标准合同》第四（六）条额外强调了境外接收方在接到当地政府部门、司法机构的数据调取要求时应立即通知个人信息处理者（境内提供方）的义务。**欧盟在SCC及TIA中也重点关注外国政府数据调取，并在SCC第15条中具体约定了境外接收方的及时通知、合理抗辩、数据最小化等义务，可供中国企业参考。**

（未完待续。敬请期待《下篇：作为协议条款的标准合同》）

2023-03-09