以标准合同进行个人信息出境的合规建议

2023-03-27

2月24日，国家网信办发布《个人信息出境标准合同办法》（以下简称“《办法》”），最终确定了以标准合同出境的个人信息出境的规则和标准合同。经过比较发现，除了少数修改，《办法》绝大部分与《个人信息出境标准合同规定（征求意见稿）》（以下简称《征求意见稿》）的条文一致。本文将结合《办法》和《个人信息保护法》，提出以标准合同进行个人信息出境的合规建议。

一、标准合同进行个人信息出境的适用对象

《办法》明确规定，必须同时符合下述条件，才能适用标准合同将个人信息出境：“（一）非关键信息基础设施运营者；（二）处理个人信息不满100万人的；（三）自上年1月1日起累计向境外提供个人信息不满10万人的；（四）自上年1月1日起累计向境外提供敏感个人信息不满1万人的。”[1]对于适用对象，《办法》与《征求意见稿》一样，但是《办法》比《征求意见稿》多了一款，即“不得采取数量拆分等手段”绕开出境安全评估，但对于何为“数量拆分”并未明确，留有空白。比如，同属一个母公司或者集团的具有独立法人资格的各个子公司分别向境外传输个人信息的是单独计算还是合并计算，这将决定把由一家公司出境改为多家子公司分别出境是否定性为“数量拆分”。对此，将留待执法进一步细化。
综上，对于数量上没有达到出境安全评估的企业，比如境内跨国公司、国内出海企业，可以选择标准合同将收集到的个人信息出境。

二、标准合同进行个人信息出境前的准备

标准合同进行个人信息出境前的准备至少包含两项工作：数据盘点和个人信息保护影响评估。

（1）数据盘点

个人信息出境的数量决定了能否适用标准合同将个人信息出境，因此，对个人信息的盘点就显得尤其必要。其中，重点就是按照《个人信息保护法》对“个人信息”以及“敏感个人信息” 的定义，结合数据处理者将个人数据出境的业务场景（比如供应链管理、人力资源管理等）统计出境的个人信息数量及相应链路等。

当然，由于刚过去的2月底是数据出境安全评估的截止日，很多具有数据处境的企业（包括很多跨国公司）已经对数据进行了盘点，相信已经对个人信息出境的数量有了内部的数据。对于比较确定不会达到数据出境安全评估标准的企业，可以提前做好签订标准合同的准备，因为《办法》的实施日是今年6月1日，并有6个月的整改期。也就是说，到2023年11月30日所有不需要进行出境安全评估申报的企业将个人信息出境的，必须签订标准合同并完成备案。[2]

（2）个人信息保护影响评估

第二个要做的准备工作就是开展个人信息保护影响评估。评估的重点包括：处理个人信息的目的、范围、方式等的合法性、正当性、必要性；出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；境外接收方承诺承担的义务，以及履行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；个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等（以下简称“数据违约”）的风险，个人信息权益维护的渠道是否通畅等；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对标准合同履行的影响。上述评估内容大部分与《数据出境安全评估办法》中规定的申报前评估内容基本一致。上述评估报告至少保存3年。[3]另外，只有准确理解上述评估重点内容的含义才能开展个人信息保

护影响评估。

a. 处理个人信息的目的、范围、方式等的合法性、正当性、必要性

“目的”、“范围”、“方式”、“合法性”、“正当性”和“必要性”这些词汇均在《个人信息保护法》中出现，但没有这样排列。《办法》当中的表述很容易让人理解为“目的”的合法性、正当性和必要性，“范围”的合法性、正当性和必要性，以及“方式”的合法性、正当性和必要性。而这很显然与《个人信息保护法》不一致。而这样的理解与《个人信息保护法》不一致，而且混乱。既然《办法》是依据《个人信息保护法》制定，那其中的术语含义及要求必须与《个人信息保护法》保持一致。

根据《个人信息保护法》第五条，合法、正当和必要其实是个人信息处理的原则，而这些原则均能对应《个人信息保护法》里具体的个人信息处理规则。合法性对应的具体规则就是不得非法收集、使用、加工、传输他人个人信息，不等非法买卖、提供或者公开他人个人信息，也不能危害国家安全和公共利益（第10条）和个人信息处理的合法性根据（比如知情同意、履行合同所必需，规定在第13条，共7种合法性基础）。正当性，是指处理个人信息的行为和程序必须是正当的，处理者“不得通过误导、欺诈、胁迫等方式处理个人信息”[4]，其对应的具体规则就是处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务（第16条），和处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理的名称或者姓名和联系方式等（第17条），以及处理者利用个人信息进行自动化决策，应当保证决策透明和结果公平、公正（第24条）。必要性是比例原则在《个人信息保护法》中的体现，[5]主要对应，收集个人信息应当限制在处理目的所需最小范围，不得过度收集个人信息（第6条第2款），处理敏感个人信息应当充分必要（第28条第2款），和个人信息保存期限应当为实现处理目的所必要的最短时间（第19条）。

根据上述法条，我们认为处理个人信息的目的要满足合法性，不能为侵犯个人隐私和破坏国家安全和公共利益为目的。范围要满足必要性，收集个人信息应当限制在处理目的所需最小范围。方式要满足正当性，处理个人信息既要行为正当又要程序正当。

b. 出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险

我们认为，这里的“规模”指的是“数量”，因为一是《征求意见稿》第五条用的是“数量”，二是结合上下文。这里的“数量”包含两方面的数量：一是个人信息的数量，一是涉及的个人信息主体数量。根据上文，“范围”是指个人信息涉及都有哪些种类。个人信息的“种类”在《个人信息保护法》和其他法律中并没有直接规定，但结合《个人信息保护法》对个人信息的定义以及对个人信息大类的分析，可以有如下对个人信息的分类：可以单独识别个人信息主体的个人信息（如姓名、地址、手机号码、银行卡号、车牌号等）、与其他信息一起可识别特定个人信息主体的个人信息（如性别、年龄、语言、职业、婚姻状况、受教育水平等）和敏感个人信息（如居民身份证号码、行踪轨迹、健康信息、生物识别信息、通信记录、账户密码等）。对于出境可能对个人信息权益带来的风险，包括安全事件的可能性和个人信息权益影响两个维度。[6]

c.境外接收方承担的义务以及履行义务的管理和技术措施、能力能否保障出境个人信息的安全

这里主要评估境外接收方对于个人信息保护都有哪些内部规章制度及人员配备、有哪些技术措施（比如加密、匿名化、去标识化、访问控制、[7]校验技术、安全传输通道、防护设备）以及这些技术措施是否有相关认证抑或是行业通用标准。而“能力”则主要体现在有效的管理及技术措施的有效。

这样的评估需要得到境外接收方的配合，需要境外接收方提供证明其管理和技术措施的资料，必要时也可与境外接收方通过各种方式进行会议、访谈了解情况。

d.个人信息出境后发生数据安全事故后个人信息权益维护的渠道是否通畅

该评估至少要评估境内数据处理者有无建立便捷的个人行使权力的申请受理和处理机制，境内数据处理者对境外数据接收方

数据安全事故的监控能力、境内数据处理者对境外发生数据安全事故的应急预案、境外数据接收方对发生安全事故所做的承诺及应急预案等。

e. 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对标准合同履行的影响

该评估主要考虑境外个人信息保护政策和法规是否阻碍标准合同的履行，重点分析境外的个人信息保护政策和法规是否对标准合同中境内数据处理者和境外数据接收方的权利义务造成履行不能或影响履行，境外是否具有落实个人信息保护的机制（比如是否具备个人信息保护的监督执法机构和司法机构等）。[8]

该评估需要分析境外个人信息保护的法律法规，必要时要取得境外接收方的相关法律意见。

三、标准合同的签订及相关条款的理解

1、标准合同模板中的条款不能修改或删除只能增加

在做完签订标准合同的准备后，境内处理者和境外接收方应当签订标准合同，《办法》规定“应当严格按照”标准合同签订，不允许修改或删除，但可以增加，增加的条款不得与标合同冲突。[9]

但是《办法》对于合同的语言并无规定，而标准合同的签订不大可能只有中文，应该还要有外文。因此，标准合同对应的外文应该如何确定？是否要经过有翻译资质的翻译机构翻译？还是仅需要双语法律工作者根据标准合同以符合外文习惯的法律语言严格对照标准合同进行转译？对于上述问题，我们建议需要双语法律工作者进行转译，因为一般只有法律人士才能理解法律语言的精确含义，才能进行准确的翻译。

2、标准合同的相关条文理解

标准合同共有九条，主要包括个人信息处理者的义务、境外接收方的义务、境外接收方所在国家或地区个人信息保护政策和法规对合同履行的影响、个人信息主体的权利、救济和合同解除。标准合同与其说是合同，不如说是给个人信息主体的的授权书，因为各条文都彰显对个人信息的保护。

（1）向境外提供个人信息的不是一律要取得个人信息主体的单独同意

标准合同第二条第（三）项只约定了两种需要个人信息主体单独同意的情形，即基于个人同意向境外提供个人信息的以及提供的信息涉及不满十四周围未成年人个人信息。根据上述约定，言外之意，就是基于其他合法性根据处理个人信息的则不需要再进过个人信息主体的再一次单独同意，即不需要个人信息主体的双重同意。比如，为订立或履行合同所必需，或者按照劳动规章制度和签订的集体劳动合同实施人力资源管理所必需。以“按照劳动规章制度和签订的集体劳动合同实施人力资源管理所必需”为例，跨国公司能否援引该同意例外直接不经员工同意直接把员工信息存储到境外服务器呢？我们认为，答案是否定的。因为境内员工一般都是与境内主体签订劳动合同，合同在国内履行，完全没有必要将员工的个人信息存储到境外服务器，只是由于跨国公司为了全球统一管理而使用人力资源管理软件，而该软件的服务器在境外，这不是《个人信息保护法》意义上的“实施人力资源管理所必需”。因此，我们建议跨国公司将员工个人信息存储到境外服务器仍然获取员工的单独同意。

（2）境外接收方超约定处理基于个人同意出境的个人信息的，应当取得个人信息主体的单独同意

标准合同中要约定处理个人信息的目的、方式和处理个人信息的种类，如果境外接收方超出约定的目的、方式和种类处理个人信息的，如果该个人信息是经过个人信息主体才到境外处理的，那么，境外接收需要再次取得个人信息主体的单独同意。如果涉及不满十四周岁未成年人个人信息的，应当取得未成年人父母或其他监护人的单独同意。标准合同条款中没有约定取得单独同意的方式，可以视情况由境内个人信息处理代为转交书面同意文件或者由境外接收方直接向个人信息主体送交同意

文件。

（3）境外接收方在接到其所在国家或地区的政府部门、司法机构提供个人信息要求的通知义务

因为涉及到个人信息的主权及安全问题，标准合同第4条第6款，约定：“境外接收方接到所在国家和地区的政府部门、司法机构关于提供本合同项下的个人信息要去的，应当立即通知个人信息处理者。”但该条并未说明通知后应该怎么处理，也并未说明境内个人信息处理者在接到通知后是否要向网信部门报告。因此，这是一个悬而未决的问题，需要在实践中不断摸索应对之策。

（4）法律适用及争议解决

标准合同第九条第二款规定，因标准合同而引起的任何争议适用中华人民共和国法律。同时，标准合同也为个人信息主体维权适用我国法律预留了空间，给个人信息主体以选择权。[10]

关于争议解决，标准合同倾向于仲裁，而且是国内仲裁。当然，境内处理和境外接收方可以选择其他仲裁机构或中国法院起诉。[11]如果选择仲裁的，仍然要对仲裁语言进行约定，由于涉及境外接收方，一般选择英语作为仲裁语言。

四、合同签订后的工作

个人信息处理者应当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。备案应当提交以下材料：标准合同（已经签好字、盖好章的合同）和个人信息保护影响评估报告。[12]当然，如果发生重大事项应当重新进行个人信息保护影响评估并重新签订个人信息出境标准合同。

对此，我们建议个人信息处理者应当对境外接收方进行定期跟踪，已确定是否发生重大变化。

[1]《个人信息出境标准合同办法》第四条。

[2]《个人信息出境标准合同办法》第十三条。

[3]《个人信息保护法》第五十六条第二款。

[4]《个人信息保护法》第五条。

[5] 程啸：《个人信息保护法理解与适用》，第81页，中国法制出版社，2021年9月。

[6]《信息安全技术 个人信息安全影响评估指南》5.6条。

[7]《个人信息出境标准合同》第二条第（五）项。

[8]《个人信息出境标准合同》第四条第二款第二项第三目。

[9]《个人信息出境标准合同办法》第六条。

[10]《个人信息出境标准合同》第六条第四款。

[11] 同上，第九条第四款。

[12]《办法》第九条。

来源：

作者：朱尉贤