HAN KUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2022 年第 7 期（总第 183 期）

新法评述

1、国家网信办正式发布《数据出境安全评估办法》

2、速览《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

新法评述

1、国家网信办正式发布《数据出境安全评估办法》

作者：段志超丨蔡克蒙丨王雨婷丨徐紫寰丨金今

2022 年 7 月 7 日，国家互联网信息办公室（“**网信办**”）正式发布《数据出境安全评估办法》（“**《评估办法》**”），细化和落实《网络安全法》第 37 条、《数据安全法》第 31 条、《个人信息保护法》第 36、38、40 条等法律中有关数据出境的规定。《评估办法》大体延续了 2021 年 10 月 29 日网信办发布的《数据出境安全评估办法（征求意见稿）》（“**《征求意见稿》**”）对数据出境从严监管的态度，采纳了《征求意见稿》提出的制度框架，但在细节处有所放松。本文旨在简析《评估办法》的要点，并提示需重点注意的事项与潜在挑战。

一、何为“向境外提供”个人信息和重要数据

根据《评估办法》第 2 条的规定，《评估办法》适用的数据出境活动系指数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的情形。此外，根据《个人信息保护法》第 4 条对个人信息的定义，向境外提供去标识化的个人信息将同样落入《评估办法》的适用范围中。

对于“向境外提供”的理解，根据网信办有关负责人在《评估办法》答记者问（“**《评估办法》答记者问**”）[1]中的介绍，《评估办法》适用的数据出境活动主要包括两大类：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外；二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用。

此外，一个备受关注的问题是，《评估办法》是否适用于《个人信息保护法》第 3 条第 2 款规定的情形，即境外主体直接从境内个人信息主体收集个人信息是否需要申报安全评估。对此《评估办法》并未明确做出规定，有待于监管后续在实践中予以明晰。从体系解释的角度看，我们倾向于认为对于个人信息而言，《评估办法》中的“向境外提供”仅指《个人信息保护法》第三章规范的境内个人信息处理者向境外提供数据的情形，换言之，境外主体直接从境内个人信息主体收集个人信息可能并不需要履行《评估办法》规定的安全评估义务。鉴于《评估办法》的适用范围仍存在一定不确定性，建议相关企业密切关注监管动态，并考虑根据全国信息安全标准化技术委员会秘书处于 2022 年 6 月 24 日正式发布的《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》，就前述直接从境内主体收集个人信息的场景完成个人信息保护认证。

二、需要申报数据出境安全评估的情况

《评估办法》第 4 条进一步明确了需要申报出境安全评估的四种情形：

- 数据处理者向境外提供重要数据；

[1] 2022 年 7 月 7 日，《数据出境安全评估办法》答记者问，具体内容请见：http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm（最后访问时间：2022 年 7 月 8 日）。

- 关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；
- 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；
- 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。

上述需要申报评估的情形有以下值得关注的要点：

（一）所有重要数据出境均需安全评估[2]

根据《数据安全法》第 31 条对网信办制定重要数据出境规则的授权，《评估办法》第 4 条将所有“数据处理者向境外提供重要数据”的情形均纳入需要申报出境安全评估的范畴，扩展了《网络安全法》第 37 条关于重要数据出境安全评估的适用范围。

（二）向境外提供个人信息的数量计算最长以两年为周期

《评估办法》整体沿用了《征求意见稿》关于“处理数量”和“提供数量”的计算标准，但“向境外提供超过 10 万人以上个人信息或者 1 万人以上敏感个人信息”自上年 1 月 1 日起累计，即统计周期最长被限于 2 年内，不再永久累计。这一调整将减轻个人信息出境规模较小的企业的合规成本。

三、本地化存储和出境安全评估的关系

一个颇具争议的问题是，达到《评估办法》处理或提供个人信息数量标准的企业是否需要履行《个人信息保护法》第 40 条规定的境内存储义务。我们认为，虽然《评估办法》并未单独提及数据存储的本地化要求，但《个人信息保护法》第 40 条明确规定“关键信息基础设施运营者”或“处理个人信息达到国家网信部门规定数量的个人信息处理者”在数据出境方面需履行两项义务，即“境内存储”在境内收集和产生的个人信息，以及在确需对外提供的情况下通过“出境安全评估”，因此理论上讲“境内存储”实质上应为达到数量门槛的企业在跨境传输之前必须履行的义务。此外，境内存储亦有助于主管部门更高效地对数据安全开展监管。考虑到《评估办法》设置的数量门槛较低，实践中在安全评估时主管部门是否会严格将“境内存储”作为通过安全评估的前提仍有待进一步观察，但考虑到数据出境安全评估冗长的流程和结果的不确定性，数据本地化（即境内存储并尽量避免数据出境）可能将成为许多企业被迫做出的抉择。

四、出境安全评估以自评估为先导

对于数据出境风险自评估的要求，《评估办法》第 5 条规定“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”。评估事项包括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；出境数据的规模、范围、种类、敏感程度以及出境行为的风险；境外接收方的保护能力；数据出境中和出境后的安全风险以及个人信息权益保障；拟订立的数据出境相关合同或者其他具有法

[2] 《评估办法》第 19 条将重要数据定义为“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”。《评估办法》并未明确列举重要数据的具体类型，因此重要数据的识别仍需要结合其他法律法规、标准予以明确。以《数据安全法》为基础，各地区、各部门负责制定本地区、本部门以及相关行业、领域的重要数据具体目录。2020 年信安委即立项开始制定相关国家标准，直至 2021 年 1 月 7 日《信息安全技术 重要数据识别指南（征求意见稿）》已经过多轮审议和修改，其将为各地区、各部门制定重要数据具体目录提供原则性指导。在行业规定中，目前汽车行业的《汽车数据安全管理若干规定（试行）》将（在汽车设计、生产、销售、使用、运维过程中涉及的）重要数据定义为“一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据”，并列举了该等重要数据的具体类型。

律效力的文件中对双方数据安全保护责任义务的约定情况等。对于个人信息出境，类似的事前内部评估同样见于《个人信息保护法》第 55 条和《个人信息出境标准合同规定（征求意见稿）》，其均要求数据处理者于个人信息出境活动前开展个人信息保护影响评估。实践中，我们认为企业可以整合内部评估流程，先行开展个人信息保护影响评估，并以此为基础按照《评估办法》的要求进而完成数据出境风险自评估。总体而言，无论企业是否属于关键基础设施运营者或达到个人信息数量门槛，企业开展事前内部评估都是个人信息和重要数据出境前必须履行的合规义务。

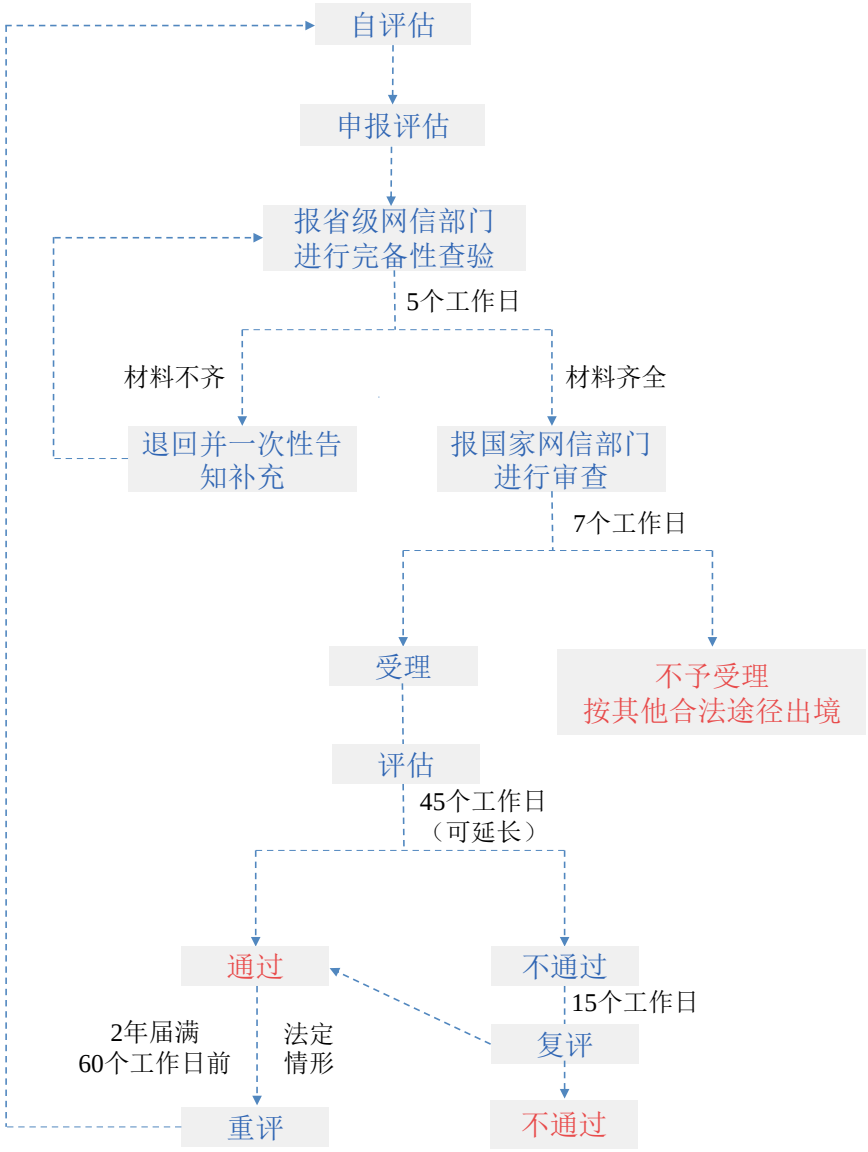
五、申报前应拟定数据出境相关合同或者其他具有法律效力的文件

数据处理者申报安全评估需提交数据处理者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。《评估办法》第 9 条指出，法律文件中应包括数据出境行为的目的、方式和数据范围；接收方的处理行为；数据在境外保存的状况；对再转移的约束性要求；接收方实质控制权和经营范围发生实质性变化，或其所在国家地区的数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形时采取的数据安全措施；违反数据安全保护义务时的补救措施、违约责任及争议解决方式；发生安全事件时的应急处置要求和个人行权渠道保障等。

《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模板可作为数据出境相关合同的模板（对个人信息出境而言）或重要参考（对重要数据出境而言）。除合同外，其他法律文件可能包括境外接收方的单方承诺函或境内外所在各方集团数据安全管理制度或政策等。但根据《评估办法》答记者问，数据处理者宜在正式通过安全评估后，再与境外接收方正式签订法律文件，或在文件中约定该等法律文件以安全评估通过为生效条件。

六、严密的评估流程

《评估办法》在第 7 条和第 11-14 条中对评估的流程进行了细致的规定，具体如下图所示。



关于申报流程有以下值得注意的要点。

（一）省级网信办形式审查

与《征求意见稿》相比，《评估办法》第 7 条补充规定了“省级网信部门应当自收到申报材料之日起 5 个工作日内完成完备性查验”。这一阶段为形式审查，申报材料齐全的将被报送至国家网信办，但如省级网信部门认为材料不齐全，则可能要求数据处理者补充直至材料齐全。

（二）删除审查延期上限

此外值得关注的是，《评估办法》第 12 条删除了原《征求意见稿》第 11 条中对延长评估的 60 个工作日上限规定。根据《评估办法》第 12 条，国家网信部门认为评估中情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。前述“延长的时间”并无明确上限，因此除正常评估需要的 45 个工作日外，安全评估可能进一步延长至超过 60 个工作日。实践中，企业的数据处理活动通常具有时效性和连续性，较长的审查期限可能对企业运营相关的各类客户数据、员工数据跨境传输带来较大的不确定性。

（三）安全评估的三种结果

国家网信办对申报的评估可能有三种结果。一是申报不予受理。对于不属于安全评估范围的，国家网信办应在收到省级网信办上报的申报材料后 7 个工作日内通知数据处理者申报不予受理，这意味着数据处理者可以通过法律规定的其他合法途径开展数据出境活动。二是通过安全评估。数据处理者可以在收到通过评估的书面通知后，严格按照申报事项开展数据出境活动。三是未通过安全评估。未通过数据出境安全评估的，数据处理者不得开展所申报的数据出境活动。这意味着数据处理者可能要改变数据出境方案重新申报（如减少数据出境范围或频率、增强数据出境后的安全保护措施）或采取数据本地化措施避免数据出境。

（四）增加异议、复评环节

《评估办法》第 13 条在《征求意见稿》的基础上额外增加了异议、复评环节，数据处理者对评估结果有异议的，可以在收到评估结果 15 个工作日内向国家网信部门申请复评，复评结果为最终结论。这一新增规定将为初次评估结果为不通过的企业提供额外的救济途径。

七、评估重点

《评估办法》规定的网信部门开展数据出境安全评估的评估重点与《征求意见稿》基本保持一致。这些评估重点中值得关注以下要点：

- **如何理解数据出境的必要性：**相较于跨境传输，可供企业选择的本地化替代性方案往往意味着显著提高的经营成本和极大的不便（如导致境内外无法协同处理某项工作、境内外分别使用不同的 IT 供应商将导致无法互联互通等），但能否以此作为数据出境的必要性在实践中可能争议较大。

- **如何评估境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响：**后续网信部门是否会像类似境外数据保护机构一样对特定国家或地区的数据保护水平做出充分性认定；抑或将委托第三方监测机构或学术机构做出评估报告；特别是在全球地缘冲突和贸易冲突加剧的情况下，一些特定国家或地区对向中国传输数据的限制或采取的其他限制措施是否会影响此项评估的结论，这些话题均有待在实践中观察与检验。

八、持续的评估监管

数据出境安全评估并非完成一次评估即可一劳永逸，《评估办法》旨在建立持续的评估和监管机制。数据处理者在数据出境评估结果的 2 年有效期内可正常开展数据出境活动。但在有效期内发生了需重新申报评估的情形，或评估结果有效期届满的，则应重新申报评估。

具体而言，数据处理者通过网信办数据出境安全评估后，在 2 年内无需就同一接收者后续的多次或连续的传输类似数据申请重新评估。然而，在下列情形中（《评估办法》第 14、17 条），数据处理者需要申请重新评估：

- 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；

- 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

- 出现影响出境数据安全的其他情形；
- 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的。

九、宽限期

《评估办法》将于 2022 年 9 月 1 日起施行。与《征求意见稿》相比《评估办法》第 20 条新增了宽限期的规定，要求《评估办法》实施前已经开展但不符合规定的数据出境活动，应在 6 个月内（即 2023 年 3 月 1 日前）完成整改。这意味着，2022 年 9 月 1 日前已经开展的、达到安全评估标准的数据出境活动虽然暂时不受影响，但应尽快补办安全评估，以确保相关出境活动后续持续开展的合规性。

十、我们的观点

《评估办法》对从中国向境外传输重要数据和一定规模的个人信息提出了前所未有的严格限制。将个人信息和重要数据出境的安全评估合二为一在一份规定中加以规范，体现了国家对大量个人信息出境带来的国家安全风险的谨慎态度与担忧。总的来说，《评估办法》的出台不仅会给在华跨国企业带来 IT 架构调整、内部组织架构调整及随之而来的巨大前期投入成本，还将产生数据出境梳理、数据跨境传输协议管理、出境数据后续境外使用持续监管等大量持续的日常合规投入。为应对《评估办法》带来的合规挑战，我们对相关企业的建议是：

- **考虑数据本地化存储：**鉴于《评估办法》对安全评估设置了较低的数量门槛，对于业务依赖于境外数据处理或集中存储的公司而言，为了避免冗长的评估程序和与此相伴的不确定性，从长远角度考虑，数据本地化可能是一个不可避免的昂贵选择。
- **完善内部制度、准备文件模板：**《评估办法》并未对安全评估设置审限上限，这将为企业数据出境带来不确定性和高昂的潜在时间成本。对于未来拟开展数据出境的企业而言，预先制定内部数据出境行为识别制度、自评估制度、准备跨境相关法律文件将是顺利推动数据出境活动的关键一环。
- **尽快开展梳理、评估工作，在宽限期内完成整改：**《评估办法》规定的生效后的宽限期为 6 个月。在此期限届满前，所有达到安全评估申报要求的企业均应尽快着手梳理相关数据出境活动，准备安全评估申报，以避免在期限届满时未完成评估无法开展数据出境活动的窘境。

2、速览《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

作者：段志超丨蔡克蒙丨胡敏喆丨张子谦丨邹奕

2022 年 6 月 30 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规定（征求意见稿）》（**“《规定》征求意见稿”**）及个人信息出境标准合同（**“标准合同”**）。《规定》征求意见稿全文共 13 条，对个人信息出境标准合同的适用范围、适用条件、主要内容等进行了明确，旨在落实《个人信息保护法》第 38 条第 3 款规定的通过订立标准合同实现个人信息出境。特别值得关注的是，《规定》征求意见稿要求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履行备案手续。尽管备案不影响合同生效和个人信息出境活动开展，但为监管机构监管个人信息出境活动提供了有力抓手。

标准合同共包括 9 条及 2 个附录，重点对个人信息处理者的义务、境外接收方的义务、个人信息主体的权利、当地个人信息保护政策法规对遵守合同条款的影响以及救济、合同解除、违约责任、法律适用和争议解决等作出了规定。

我们将在下文简要总结和《规定》征求意见稿以及标准合同的主要内容，并为企业在实践中落地应用标准合同提供建议。

一、个人信息出境标准合同的适用范围

（一）可通过标准合同实现个人信息出境的场景

《规定》征求意见稿第 4 条规定了个人信息处理者通过签订标准合同向境外提供个人信息所应具备的全部 4 项条件，包括：

1. 非关键信息基础设施运营者；
2. 处理个人信息不满 100 万人的；
3. 自上年 1 月 1 日起累计向境外提供未达到 10 万人个人信息的；
4. 自上年 1 月 1 日起累计向境外提供未达到 1 万人敏感个人信息的。

上述 4 项条件将根据《个人信息保护法》以及后续将要出台的数据安全评估办法必须向网信部门申请数据出境安全评估的情形排除在外。但这不意味着申请网信部门数据出境安全评估的情况无需签署标准合同，而是企业无法单纯通过签署标准合同完成个人信息出境，还需要在标准合同基础上申请网信部门安全评估。

值得注意的是，上述第 2 项、第 3 项、第 4 项条件所规定的数量标准与此前 2021 年出台的《数据出境安全评估办法（征求意见稿）》（**“《评估办法》征求意见稿”**）中的数量标准保持一致，预计后续正式出台的数据出境安全评估办法也将大概率采纳这一标准。而上述第 3 和第 4 项条件对此前个人信息处理者普遍关心的“累计数量”的时间跨度标准做出了澄清，明确向境外提供个人信息或敏感个人信息的数量自上年 1 月 1 日起进行计算。以 1-2 年为个人信息数量累计的周期在一定程度上有利于个人信息出境规模较少的企业利用标准合同这一相对便利的机制实现个人信息出境。

（二）似不适用境外主体直接收集境内个人信息

境外主体直接收集境内自然人个人信息并不属于境内个人信息处理者向境外提供个人信息的情况，不属于《个人信息保护法》第 38 条和《规定》征求意见稿意义上的“个人信息出境”，因此似无法适用标准合同。但如果境外主体满足《个人信息保护法》第 3 条第 2 款的规定，其收集并处理境内自然人个人信息仍属于“个人信息跨境处理活动”，可按照《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》规定由其在境内设置的专门机构或指定代表申请认证，并承担法律责任。

二、个人信息出境标准合同的主要内容

本次发布的标准合同共 9 条及 2 个附件，分别规定了个人信息处理者、境外接收方的权利义务并明确了个人信息主体的权利。从内容上看，标准合同无疑借鉴了欧盟监管机关依据 GDPR 发布的最新版标准合同（Standard Contractual Clause，“**SCC**”），但同时根据《个人信息保护法》的要求体现了颇多原创性规定。最为明显的是标准合同在整体架构上最新版 SCC 一样区分控制者与控制者、控制者与处理者、处理者与控制者、处理者与处理者等四种模式，而是在具体条款设计上对境外接收方作为独立个人信息处理者或受托方做出了适当地区别规定。

（一）基本事实情况

标准合同要求境内个人信息处理者和境外接收方对个人信息出境的基本事实情况在附录一中做出明确约定，包括合同惯常应具备的个人信息处理者和境外接收方的基本信息，如名称、地址、联系人姓名、联系方式等，以及需在附件说明的出境数据的基本情况，如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。

（二）个人信息处理者的义务

标准合同第 2 条明确了个人信息处理者应当履行的义务，除重申了现行法律法规规定的个人信息处理者需履行的关于个人信息出境的法定义务外，还要求个人信息处理者对境外接收方承担监督管理者责任。从第 2 条规定的个人信息处理者义务以及第 9 条第 6 款规定的个人信息处理者对个人信息主体的任何损失负责等条款来看，个人信息处理者将成为个人信息出境的主要责任方以及监管机关开展监管执法的首要对象。具体而言，个人信息处理者的义务包括：

1. **最小必要原则：**出境个人信息的范围应以实现处理目的所必需为限。

2. **告知：**除《个人信息保护法》第 39 条所要求告知的境外接收方的姓名/名称、联系方式，出境目的、出境方式、个人信息种类、个人向境外接收方行使法定权利的方式和程序之外，标准合同还要求个人信息处理者向个人信息主体告知境外接收方再次对外提供个人信息的接收方、出境后存储时间、存储地点以及其他附录一所约定的信息。此外，标准合同还要求个人信息处理者向个人信息主体告知个人信息主体将成为标准合同的第三方受益人，若个人信息主体在 30 天内未明确拒绝，则可依据标准合同享有第三方受益人的权利。

3. **单独同意：**标准合同要求个人信息处理者获得个人信息主体的单独同意，但同时明确“相关法律法规规定不需要取得个人单独同意的除外”，为企业依据同意之外的其他法律基础实现数据出境预留了一定空间。

4. **合理审查境外接收方的合规情况：**个人信息处理者应采取合理努力确保境外接收方能履行安全保障义务并采取必要技术和管理措施保护个人信息安全，需综合考虑出境个人信息的敏感程度与规

模、个人信息在境外的存储地点与期限等多方面因素。

5. **向境外接收方提供中国法律规定和技术标准的副本：**若境外接收方要求，个人信息处理者有义务向境外接收方提供中国相关法律规定和技术标准的副本。

6. **答复监管询问：**原则上应由个人信息处理者负责答复监管机构的询问，但双方约定由境外接收方负责答复的除外。需要注意的是，若境外接收方未在规定期限内答复，则仍需由个人信息处理者负责答复。

7. **开展个人信息保护影响评估：**个人信息处理者应当承诺已经完成个人信息保护影响评估（具体可参见本文第三部分）并保存个人信息保护影响评估报告至少 3 年。

8. **向个人信息主体提供合同副本：**个人信息主体有权要求个人信息处理者提供个人信息处理者与境外接收方签订的标准合同副本，但若合同内容涉及商业秘密或其他机密，个人信息处理者可对涉密信息进行必要遮盖，但应当向个人提供有效摘要确保其可以理解合同内容。

9. **合规证明举证：**个人信息处理者负有证明其已履行合同义务的举证责任。

10. **向监管提供境外接收方合规证明材料：**个人信息处理者应当根据相关法律法规的要求，向监管机构提供能够证明境外接收方遵守本合同中规定义务的信息。为此，结合第 3 条第 10 款的规定，个人信息处理者有权要求查阅相关数据文件和文档或者对涉及的处理活动进行审计。

（三）境外接收方的义务

标准合同通过将《个人信息保护法》等相关法律法规下的个人信息保护合规义务转化为境外接收方的合同义务，从而确保不受《个人信息保护法》直接管辖的境外主体可以对出境个人信息提供《个人信息保护法》所要求的保护水平。此外，标准合同还规定了境外接收方配合境内个人信息处理者接受中国监管机构检查的义务和责任，从而保障境内个人信息处理者得以有效承担监督与检查责任。境外接收方的具体义务包括：

1. **处理限于约定范围：**境外接收方对个人信息的处理应当严格限制在约定范围内，除非另行取得个人信息主体的同意。

2. **向个人信息主体提供合同副本：**个人信息主体有权要求境外接收方提供所签订的标准合同副本，但若合同内容涉及商业秘密或其他机密，境外接收方可对涉密信息进行必要遮盖，但应当向个人提供有效摘要确保其可以理解合同内容。

3. **最小必要原则：**出境个人信息的范围以实现处理目的所必需为限。

4. **存储期限最短原则：**存储个人信息的期限为实现处理目的最短时间，除非取得个人信息主体关于存储期限的单独同意。

5. **保障处理安全原则：**境外接收方需采取技术和管理措施保障个人信息安全，并确保其授权处理个人信息的人员履行保密义务，建立最小授权的权限管控机制。

6. **安全事件应急响应：**若发生个人信息泄露等安全事件，境外接收方应及时采取补救措施减少对个人信息主体的不利影响，并立即通知个人信息处理者，并根据中国相关法律法规要求报告中国监管机构以及通知个人信息主体。同时，境外接收方需记录并留存安全事件事实与影响（包括所采取的补救措施）。

7. **个人信息再传输严格受限：**境外接收方原则上不应再向境外第三方提供所接收的个人信息，除非业务确有需要且满足如下要求：

- 已告知个人信息主体第三方身份、联系方式、处理目的、方式、个人信息种类及个人行使权利的方式和程序，并取得单独同意（法律法规另有规定的除外），涉及敏感个人信息的已向个人告知传输敏感个人信息的必要性及对个人的影响。若难以告知或难以取得单独同意，则境外接收方应及时告知个人信息处理者并请求其协助告知个人信息主体或协助取得个人的单独同意；
- 与第三方签订书面协议，确保第三方对个人信息的保护水平不低于中国相关法律法规规定的保护标准；
- 承担因再提供而可能导致的个人信息主体损害的连带责任；
- 向个人信息处理者提供境外接收方与第三方签订的协议副本。

8. **自动化决策要求的重申：**若存在利用个人信息进行自动化决策的场景，与《个人信息保护法》第 24 条的要求一致，需保障透明度与结果公平公正，拒绝交易价格和条件的差别待遇。在营销场景下向个人提供不针对个人特征的选项或便捷的拒绝方式。

9. **配合个人信息处理者的义务：**向个人信息处理者提供证明境外接收方履行合规义务的必要信息和材料，配合相关审计活动。

10. **个人信息处理活动记录及保存义务：**境外接收方需对个人信息处理活动进行记录并保存记录至少 3 年。同时，标准合同在此基础上特别要求境外接收方有义务按照相关法律法规要求直接或者通过个人信息处理者向监管机构提供相关记录文件。

11. **同意接受监管机构的监督管理：**境外接收方需同意在标准合同实施的程序中接受监管机构的监督管理（包括答复询问、配合调查、服从监管机构采取的措施或决定、提供采取必要行动的书面证明等）。

除上述义务外，如境外接收方系接受个人信息处理者委托在境外处理境内个人信息，还需遵守以下特殊要求：

1. 委托关系结束后，删除或匿名化个人信息之后，向个人信息处理者提供审计报告；
2. 在发生个人信息泄露事件时，由个人信息处理者通知个人信息主体；
3. 若境外接收方需转委托第三方处理，则需征得个人信息处理者的同意，确保第三方在标准合同范围内处理个人信息并且对第三方活动进行监督。

（四）个人信息主体的权利和救济

1. 权利范围

标准合同第 5 条明确了个人信息主体享有《个人信息保护法》第 4 章规定的主要权利，包括：知情权、决定权、限制或拒绝他人对其个人信息进行处理的权利、查阅权、复制权、更正与补充的权利、删除权，以及要求对其个人信息处理规则进行解释说明的权利，但暂未明确列明仍待网信办明确具体行使条件的“将个人信息转移至指定的个人信息处理者”的权利。

2. 行使对象

程序方面，标准合同允许个人信息主体（1）请求个人信息处理者采取适当措施实现，即通过境内个人信息处理者行使权利（境外接收方有义务协助），或（2）直接向境外接收方提出请求。

3. 境外接收方有权拒绝不合理行权，但应告知救济途径

标准合同第 5 条第 4 款规定，如个人信息主体提出过多或不合理要求，尤其是具有重复性的要求，境外接收方可在考虑到要求获准的执行和操作成本后，可以收取合理的费用，或拒绝按其要求行事。但如境外接收方拟拒绝个人信息主体的请求，应告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机构提出投诉、寻求司法救济的途径。这也是网信办在其发布的文本中首次对个人信息主体权利作出限制性的规定，或将有助于个人信息处理者应对个人信息主体不合理的权利请求。

4. 个人信息主体享有的救济和第三方受益人条款

标准合同明确境外接收方应确定联系人接受、处理境内个人信息主体投诉的义务、向个人信息处理者及时通知与个人信息主体争议的义务，并规定个人信息主体有权就标准合同产生的争议向我国监管机构或法院寻求救济，境外接收方接受我国监管机构或法院的管辖。

标准合同参考 SCC，将个人信息主体规定为合同的第三方受益人。个人信息主体有权直接向个人信息处理者和境外接收方任何一方主张并要求履行标准合同项下与个人信息主体权利相关的条款，例如：个人信息处理者和境外接收方的部分义务（如告知同意、最小必要、数据安全保护等）、评估当地个人信息保护政策法规对遵守本合同条款的影响、合同解除等，并在个人信息处理者或境外接收方未能履行合同义务的情况下，向中国有管辖权的人民法院提起诉讼并要求其承担违约责任。

（五）确保数据接收方所在地法律不会影响合同履行

2021 年，欧盟监管机关为回应欧盟法院在 Schrems II 案中所作的判决，进一步说明了 SCC 的使用条件，要求通过签署 SCC 向欧盟境外传输个人数据的控制者事先评估第三国的立法与实践，重点关注公共机构获取数据的立法与实践并确定需要采取的补充措施。标准合同第 4 条亦借鉴了这一做法，要求双方应当采取合理努力了解境外接收方所在国家或者地区的个人信息保护政策法规（包括任何提供个人信息的要求或授权公共机关访问个人信息的规定），确保当地法律不会影响境外接收方履行标准合同规定的义务。

标准合同第 4 条第 2 款明确了开展上述评估时需要考虑的因素，包括：

1. 出境的具体情况，包括涉及传输的个人信息的类型、数量、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方保存的期限、个人信息处理目的、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生数据安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息请求及境外接收方应对的情况；

2. 境外接收方所在国家或者地区的个人信息保护政策法规，包括：（1）该国家或地区现行的个人信息保护法律法规及普遍适用的标准情况；（2）该国家或地区加入的区域或全球性的个人信息保护方面的组织，以及所做出的具有约束力的国际承诺；（3）该国家或地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

3. 境外接收方安全管理制度和技术手段保障能力。

此外，标准合同还规定了其他与上述评估配套的配合义务，包括境外接收方应尽最大努力为个人信息处理者提供了必要的相关信息，双方应记录评估过程和结果，境外接收方应在知道其所在国家或地区的个人信息保护政策法规发生变化导致其无法履行本合同时立即通知个人信息处理者。

（六）合同解除

标准合同第 7 条规定，（1）境外接收方严重或持续违反本合同规定的义务，或（2）境外接收方破产、解散或清算等，个人信息处理者可以解除合同。此外，（1）因境外接收方违反合同规定的义务，个人信息处理者暂停向境外接收方传输个人信息的时间超过一个月；（2）境外接收方遵守本合同将违反其所在国家的法律规定；（3）根据境外接收方的主管法院或监管机构作出的不能上诉的终局性决定，境外接收方或个人信息处理者违反了本合同的规定；（4）在监管机构按照相关法律法规作出个人信息出境相关的决定导致标准合同无法执行的情况下，任何一方可以解除合同。

需要说明的是，根据第 7 条第 4 款和第 5 款的规定，标准合同的解除并不免除其在个人信息处理过程中的个人信息保护义务，境外接收方应及时返还、销毁或匿名化处理其根据标准合同所接收到的个人信息，并提供已经销毁或者匿名化处理的审计报告。

（七）违约责任

除惯常的违约责任外，标准合同第 8 条针对一方违约对个人信息主体造成的损害赔偿责任的承担做出了约定：

1. 个人信息处理者和境外接收方对因违反本合同而共同对个人信息主体造成的任何物质或非物质损害负责的，个人信息处理者和境外接收方应对个人信息主体承担**连带责任**。

2. 如果一方（**“赔偿方”**）因另一方（**“被追偿方”**）对违反本合同的行为对个人信息主体承担连带责任且赔偿方承担的连带责任超过其应承担的责任份额，则赔偿方有权向被追偿方追偿。

尽管有上述违约责任的划分机制以及双方之间的责任追偿机制，但考虑到个人信息主体在实践中可能难以直接向境外接收方求偿，标准合同第 8 条第（6）款规定，个人信息处理者应就境外接收方因违反标准合同而对个人信息主体造成的任何物质和非物质损失向个人信息主体负责，个人信息主体有权向个人信息处理者主张损害赔偿责任。因此，在境外接收方违约的情况下，个人信息处理者将可能首先需要承担赔偿责任，然后再向境外接收方进行追偿。

（八）争议解决和法律适用

标准合同明确规定，本合同适用于中华人民共和国相关法律法规。而对于争议解决方式，标准合同允许双方选择仲裁或者向中国有管辖权的人民法院提起诉讼。对于仲裁机构的选择，标准合同允许双方将争议提交至中国国际经济贸易仲裁委员会、中国海事仲裁委员会、北京仲裁委员会（北京国际仲裁中心）以及其他《承认及执行外国仲裁裁决公约》成员的仲裁机构。这意味着标准合同允许双方选择其他纽约公约缔约国仲裁机构作为合同争议解决方式，为境外接送方寻求中立仲裁地留下了空间。

三、使用个人信息出境标准合同需采取的“配套措施”

《规定》征求意见稿同时明确了在通过签订标准合同的方式向境外提供个人信息时，个人信息处理者需要履行的配套合规义务和程序性规定。此外，为履行标准合同条款下的义务，个人信息处理者还需要进行一系列配套准备工作。本部分简单梳理了个人信息处理者为使用标准合同条款需采取的“配套措施”，具体如

下：

（一）合同签订前

1. **梳理既有个人信息处理实践，判断是否可以通过签订标准合同的方式向境外提供个人信息。**个人信息处理者应当根据《规定》征求意见稿第 4 条的规定，从“是否为关键信息基础设施运营者”、“处理个人信息的数量”以及“自上年 1 月 1 日累计向境外提供个人信息和敏感个人信息的数量”等方面，判断个人信息处理者是否可以通过签订标准合同的方式向境外提供个人信息。

2. **梳理此次个人信息出境的具体事实情况。**个人信息处理者应当明确此次个人信息出境所涉及的个人信息主体类别、个人信息出境目的、数量、方式、个人信息类别、敏感个人信息类别、境外接收方提供个人信息的接收方、境外存储时间、存储地点，境外接收方是否进行转委托或开展再传输活动以及其他相关事项，以便履行《规定》征求意见稿第 5 条规定的开展个人信息保护影响评估的义务并在签署合同时填写标准合同附录一所需的信息。

3. **检查自身合规措施。**考虑到标准合同要求个人信息处理者就其承担的各项义务作出陈述、保证和承诺，一旦个人信息处理者在后续个人信息出境中出现违约行为，不仅可能受到监管机关的调查乃至处罚，还可能会被境外接收方要求承担相应的违约责任，因此，建议个人信息处理者在向签署个人信息出境标准合同前，对照《个人信息保护法》及《规定》征求意见稿第 2 条个人信息处理者的义务，特别是告知和单独同意机制，为需要事先开展的个人信息保护影响评估做好准备。

4. **事先评估境外接收方的个人信息保护能力。**由于标准合同将个人信息处理者作为监管机关管理个人信息出境活动的首要对象且境外接收方的个人信息保护能力可能影响到个人信息保护影响评估的结果，建议个人信息处理者在开展个人信息出境活动前对照《规定》征求意见稿第 3 条境外接收方的义务逐一评估境外接收方的个人信息保护能力，降低个人信息出境的合规风险。

5. **考察和评估当地个人信息保护政策法规对遵守本合同条款的影响。**根据标准合同第 4 条的要求，双方应当通过合理努力了解境外接收方所在国家或者地区的个人信息保护政策法规是否会给境外接收方履行标准合同规定义务带来障碍。参考 GDPR 的有关实践，个人信息处理者可以编制接收方所在国家或地区问卷清单，通过境外接收方或者当地律师了解当地个人信息保护的政策法规并结合前述了解到的接收方的个人信息保护能力作出评估。

6. **开展个人信息保护影响评估并留存记录。**在前述第（2）-（5）步的基础上，按照《个人信息保护法》第 55 条和《规定》征求意见稿的要求开展个人信息保护影响评估并留存记录至少 3 年[3]。同时，结合《个人信息保护法》、《评估办法》征求意见稿以及《信息安全技术 数据出境安全评估指南（征求意见稿）》的规定，个人信息处理者的评估可以分为两步：出境目的评估与安全风险评估。在出境目的评估阶段，个人信息处理者可以对出境目的是否同时满足合法性、正当性和必要性做出判断；在安全风险评估阶段，个人信息处理者可以对个人信息的类型、数量、范围、敏感程度、

[3] 个人信息保护影响评估需重点评估以下内容：（1）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；

（2）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；

（3）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；

（4）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；

（5）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；

（6）其他可能影响个人信息出境安全的事项。

技术安全保障情况进行评估，并结合数据发送方的数据安全保护能力以及数据接收方的安全保护能力做出综合判断。

（二）合同签订后

1. **在合同生效之日起 10 个工作日内向省级网信部门履行备案手续。**《规定》征求意见稿第 7 条规定，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：（一）标准合同；（二）个人信息保护影响评估报告。需要说明的是，第 7 条第 2 款同时明确，标准合同生效后个人信息处理者即可开展个人信息出境活动，即开展个人信息出境活动并不以个人信息处理者履行完毕备案手续为前提，但个人信息处理者应当对所备案材料的真实性负责。

2. **向个人信息主体提供标准合同副本。**根据标准合同第 2 条在个人信息主体要求个人信息处理者提供个人信息处理者与境外接收方签订的标准合同副本时向其提供合同副本，或为保护商业秘密等目的对合同内容进行调整后向其提供，但应当承诺向个人提供有效摘要以帮助个人了解合同内容。

3. **更新隐私政策或其他告知文本。**为履行向个人信息主体提供合同副本，提供便利的权利行使机制等义务，个人信息处理者需更新隐私政策或其他告知文本，明确告知个人获得标准合同副本和向个人信息处理者或境外接收方行使权利的途径。

4. **持续监测个人信息出境情况，在出现规定情形时与境外接收方重新订立标准合同。**《规定》征求意见稿第 8 条规定了个人信息处理者应当重新签订标准合同并备案的三种情形，包括：（一）向境外提供个人信息的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点和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；（二）境外接收方所在国家或者地区的个人信息保护政策法规发生变化等可能影响个人信息权益的；（三）可能影响个人信息权益的其他情况。

5. **留存个人信息出境记录及相关的书面文件。**考虑到个人信息处理者需承担证明已经履行标准合同义务的举证责任，个人信息处理者应当注意留存和归档与个人信息出境有关的文件记录，例如：对当地个人信息保护政策法规的评估记录、个人信息保护影响评估记录。

6. **接受监管机关检查。**《规定》征求意见稿第 11 条规定，省级以上网信部门发现通过签订标准合同的个人信息出境活动在实际处理过程中不再符合个人信息出境安全管理要求的，应当书面通知个人信息处理者终止个人信息出境活动。个人信息处理者应当在收到通知后立即终止个人信息出境活动。此外，《规定》征求意见稿第 12 条还就个人信息处理者未履行备案程序或者提交虚假材料进行备案、未履行标准合同约定的责任义务侵害个人信息权益造成损害、出现影响个人信息权益的其他情形规定了相应的处罚，即：由省级以上网信部门依照《个人信息保护法》的规定，责令限期改正；拒不改正或者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。

四、总结与展望

简言之，标准合同虽然为个人信息处理者提供了无需网信部门安全评估即可向境外传输个人信息的机制，但其适用并不轻松。个人信息处理者需做足准备，建立包含告知同意、用户权利行使、数据安全保护、境外接收方监督管理、接收方所在国家地区法律调研追踪等数据跨境合规治理机制，方可实现个人信息顺利出境。

此外，自《个人信息保护法》确立个人信息出境基本制度框架以来，网信办已经于去年发布《评估办法》征求意见稿，信息安全标准化技术委员会也在今年发布《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》。随着相关制度逐渐落地，我国个人信息出境的合规方案将逐渐明晰并具有可操作性，无论是具有海外业务的中国企业还是在华运营的外资企业均应密切关注相关立法动态，尽早设计合理可行的个人信息出境合规方案。

特别声明

汉坤律师事务所编写《汉坤专递》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤律师事务所的下列人员联系：

北京　金文玉　律师：

电话：　+86 10 8525 5557

Email：　wenyu.jin@hankunlaw.com

上海　曹银石　律师：

电话：　+86 21 6080 0980

Email：　yinshi.cao@hankunlaw.com

深圳　王哲　律师：

电话：　+86 755 3680 6518

Email：　jason.wang@hankunlaw.com

海口　朱俊　律师：

电话：　+86 898 3665 5000

Email：　jun.zhu@hankunlaw.com

武汉　马姣　律师：

电话：　+86 27 5937 6200

Email：　jiao.ma@hankunlaw.com

香港　陈达飞　律师：

电话：　+852 2820 5616

Email：　dafei.chen@hankunlaw.com