数据流动的分寸：评析《数据出境安全评估办法》

作者：杨建媛

2022年7月7日，国家互联网信息办公室（“**国家网信办**”）发布了《数据出境安全评估办法》（“**《办法》**”），并回答了记者的相关提问（“**答记者问**”）。《办法》构建了涵盖重要数据、个人信息的数据出境安全评估制度（“**安全评估**”），细化落地了《网络安全法》《数据安全法》《个人信息保护法》中有关安全评估的规定。

总体观之，安全评估立足于国家安全的宏观站位，从处理者性质、数据量级、出境方式等维度划定了较广的适用范围，并界定了评估项、法律文件等实质内容。此外，《办法》进一步明确了安全评估的程序性事宜，为其落地执行奠定了基础。安全评估可能对企业的数据出境活动甚至业务整体运营产生较大影响，建议企业尽快开展数据合规工作，提前规划数据出境的整体布局。

一、数据出境安全评估的宏观站位：立足于国家安全

个人信息是所有企业均涉及的处理对象，也是目前大部分企业的关注焦点。安全评估固然是《个人信息保护法》的出境条件之一，《办法》也有保护个人信息权益的意旨，但值得注意的是，《办法》更高的站位在于维护国家安全。出境重要数据必须通过安全评估同样说明安全评估系立足于国家安全。

从维护国家安全的视角，有助于企业更准确地理解安全评估。一方面，企业在盘点自身的数据资产与处理活动、评估相关风险时，不应仅着眼于个人权益的微观层面，还应考虑国家安全、公共利益的宏观层面。另一方面，监管机构在进行安全评估时，一开始确实可能是广泛的摸底排查，但在实践中终将聚焦于具有宏观影响、尤其是国家安全风险的特殊业务场景，长期而言并不会过度影响企业的正常业务经营。

立足于国家安全的另一个典型制度为网络安全审查，尤其是针对赴国外上市的场景，与安全评估在适用门槛（100万人个人信息）、评估项（国家安全风险）、审查机构（国家网信部门）等方面颇有共通之处。此外，向境外执法或司法机构提供存储于中国境内数据的审查批准，以及对人类遗传资源、地理测绘信息的出境管理，同样立足于国家安全，但相对于安全评估更具针对性。当多个数据出境监管机制出现竞合时，或可在通过上述特定审查的前提下，适当豁免安全评估。

二、适用范围：特定数据、特定主体、特定量级

《办法》明确了安全评估的适用范围，细化了上位法的规定，并与《个人信息出境标准合同规定（征求意见稿）》相调和。但在落地执行过程中，《办法》的适用范围仍存在一些不确定性。

1.特定数据：重要数据

只要出境所涉的数据在定性上构成“重要数据”，则无论其数量如何，无论数据处理者的性质如何，均适用安全评估。

《办法》在我国通用且生效的法律法规层面首次定义了“重要数据”，即“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”。该定义立足于数据安全事件可能造成的危

害，且限缩于宏观层面的影响，并未包含对组织和个人合法权益的影响。

但是，重要数据的具体范围尚不清晰。《网络数据安全管理条例（征求意见稿）》《信息安全技术 重要数据识别指南（征求意见稿）》尝试对重要数据进行列举，但该等规定仍未定稿发布、且立法思路也经历更迭。一方面，有待各地区、各部门确定重要数据具体目录；另一方面，有待我国就重要数据的识别规则形成基本共识。在此之前，建议企业从严把握重要数据的认定，毕竟国家安全无小事。

2.特定主体

（1）关键信息基础设施运营者

只要出境所涉的数据处理者在定性上构成“关键信息基础设施运营者”，则无论其出境的重要数据或个人信息的数量如何，均适用安全评估。

根据《关键信息基础设施安全保护条例》，如果企业的网络设施、信息系统被认定为“关键信息基础设施”，企业将会接到监管机构的通知。

（2）处理100万人以上个人信息的数据处理者

根据体系解释，《办法》中“处理100万人以上个人信息的数据处理者”即为《个人信息保护法》中“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”，不仅适用安全评估，还应将在境内收集和产生的个人信息存储在境内（“**本地化**”）。

3.特定量级：自上年1月1日起累计向境外提供10万人个人信息或1万人敏感个人信息的数据处理者

《办法》新增了已出境数据的累计期限，最多不超过2年，放行了只涉及少量、临时出境活动的处理者。

《办法》并未规定个人信息、敏感个人信息可通过折算（如1万敏感个人信息=10万个人信息）达到门槛，但根据常理，敏感个人信息属于个人信息，至少可以按1:1计入个人信息的数量。

此外，根据《个人信息保护法》，匿名化信息不属于个人信息，而去标识化信息仍属于个人信息。企业在业务场景中往往无法实现匿名化（即，无法识别特定自然人且不能复原），而只能达到去标识化。我国现行法并未豁免去标识化信息，但去标识化的确可以降低实质风险，可作为企业通过安全评估的支撑点之一。

三、适用范围：从数据、方式、主体界定“出境”

我国现行法并未明确定义“数据出境”，且用词也有所不同，如《网络安全法》的“向境外提供”，《数据安全法》的“出境”，《个人信息保护法》的“跨境提供”和“向境外提供”。参考2017年的《个人信息和重要数据出境安全评估办法（征求意见稿）》《信息安全技术 数据出境安全评估指南（征求意见稿）》，“数据出境”一般被定义为网络运营者将在我国境内运营中收集和产生的个人信息和重要数据，提供给境外的机构、组织或个人。

在答记者问中，国家网信办进一步解释了“向境外提供”的情形包括：（1）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；（2）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。这一解释颇有启发，但仍存在一些疑问。

1.对于数据，限定于在境内运营中收集和产生的重要数据、个人信息，可以理解为不包含纯境外数据的过境或仅对纯境外数据加工后再出境。

2.对于方式，“出境”的范围较广，既包括将数据传输、存储至境外，也包括从境外可以访问、调用境内数据的情形，即无论数据的物理位置而采用可获得性标准（类似于欧盟的“make available”）。但在实践中，访问、调用的实质风险一般低于物理跨境，因为境内的数据处理者可以随时中断访问权限。

3.对于主体，《办法》提及的两类主体为数据处理者（作为数据提供方）和境外接收方，但存在两点困惑：

（1）当受托方（如云平台）作为数据提供方时，是否由委托方申报安全评估并承担责任。“数据处理者”在生效法律下尚无定义，但《个人信息保护法》将“个人信息处理者”定义为在个人信息处理活动中自主决定处理目的、处理方式的组织、个人，《网络数据安全管理条例（征求意见稿）》也要求数据处理者能自主决定处理目的、处理方式，可以理解为不包含受托方。

（2）如果境外数据处理者直接收集、传输数据，是否适用安全评估。考虑到《个人信息保护法》要求受域外管辖的境外数据处理者在我国境内设立专门机构或指定代表，《办法》也未将“数据处理者”限定在境内，能否排除境外数据处理者对安全评估的适用有待观察。

四、自评估、监管评估相结合，全面拆解数据出境安全风险

安全评估需“两步走”：先由企业自行开展数据出境风险“**自评估**”，再由国家网信部门开展“**监管评估**”。

无论企业通过安全评估、专业认证、标准合同等任一路径出境个人信息，监管机构均要求企业开展自评估，并提交监管机构审查或备案。在《个人信息保护法》对于个人信息保护影响评估（“**PIA**”）的通用要求之外，不同出境路径的配套制度分别对评估项进行细化甚至增加，但本质上仍有相通之处，而安全评估额外强调数据出境对国家安全的影响。

安全评估的自评估主要包括如下维度和内容：

评估维度	评估内容
出境事由合法正当	数据的规模、范围、种类、敏感程度
	处理的目的、范围、方式
出境风险相对可控（安全风险角度）	影响对象：国家安全、公共利益、个人或组织合法权益
	时间阶段：出境中、出境后（包括再转移）
	风险类型：数据遭到篡改、破坏、泄露、丢失、转移，被非法获取、非法利用
出境风险相对可控（境外接收方角度）	实质能力：境外接收方履行数据安全保护责任义务的能力、管理和技术措施
	法律约束：拟订立的法律文件中对数据安全保护责任义务的约定

安全评估中的监管评估覆盖了自评估的内容，并额外增加如下评估项：

（1）境外接收地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。这既可能上升至该法域的宏观安全水平（类似于欧盟的充分性认定），也可能仅限于对本次数据出境的影响（类似于欧盟的传输影响评估/TIA）。

（2）境外接收方的数据保护水平是否达到我国法律、行政法规的规定和强制性国家标准的要求。这在《个人信息保护法》的同等保护水平的基础上，额外增加了强制性国家标准，进一步细化、提升了对境外接收方的要求。

五、明确程序性事宜，保障安全评估的落地执行

相较于征求意见稿，《办法》进一步明确了安全评估的程序，为其落地执行奠定了基础。其中，值得重点关注的程序性规定包括：

1.监管机构的内部分工：一方面，由省级网信部门对申报材料进行完备性查验，合理分配网信部门的工作负担；另一方面，由国家网信部门进行安全评估，切实保障评估标准的一致性，避免出现数据出境的高地与洼地。此外，《办法》保留了网信部门与国务院有关部门、专门机构的合作，但删除了前一版征求意见稿中关于“征求相关行业主管部门意见”的规定。

2.监管评估的时间预期：在申报通过完备性查验（5个工作日内）、并予以受理（7个工作日内）后，安全评估一般在45个工作日内完成。但情况复杂或需要补正材料的，可以适当延长时间，且《办法》删除了前一版征求意见稿中“一般不超过60个工作日”的限制，延长时间更难预估。

3.申报安全评估的所需材料：（1）申报书，一般为制式文件；（2）自评估报告，参考网络安全审查，国家网信办可能会发布模板，但报告的颗粒度仍可能存在弹性空间；（3）双方拟订立的法律文件，且国家网信办建议企业先申报、后签订，或附生效条件（通过安全评估），以避免未通过评估而造成损失；（4）其他材料。

4.申报安全评估的可能结果：（1）不予受理，可以理解为该次数据出境不适用安全评估，但个人信息出境仍需满足专业认证或标准合同；（2）通过安全评估，企业应严格按照申报事项开展数据出境活动，有效期为2年，但有效期内情况发生变化而影响出境数据安全的，应重新申报；（3）未通过安全评估，企业不得开展其所申报的数据出境活动，且鉴于安全评估的优先地位，企业也无法适用专业认证或标准合同。此外，《办法》新设了复评程序，给企业提供了一次异议机会，复评结果即为最终结论。

5.《办法》的宽限期及溯及力：《办法》自2022年9月1日起施行，施行前已经开展的数据出境活动，应自施行之日起6个月内完成整改。一方面，《办法》预留了宽限期，为企业的合规工作提供了合理的准备时间；另一方面，《办法》可能溯及其施行前已开展的数据出境活动，至少对于目前仍在持续的数据出境活动，企业应依法申报安全评估。

六、面对安全评估，建议企业尽快启动数据合规工作

近期，我国关于数据出境的配套规则纷纷出台或征求意见，包括安全评估、个人信息出境标准合同（点击查看解读文章）、个人信息跨境处理活动安全认证（点击查看解读文章）。

尤其是即将正式实施的安全评估，一般需要57个工作日（5+7+45）、近3个月自然日完成。根据《办法》，对于需要开展安全评估的企业，如果2023年3月1日前未通过安全评估或未收到评估结果，则可能因此影响数据出境、甚至业务的连续运营。基于此，建议企业在《办法》施行前即开展准备工作，如需申报，在《办法》于今年9月1日起施行后尽早申报较为稳妥。

面对安全评估，企业可以提前开展的数据合规工作主要包括：

1.盘点数据资产与出境活动。企业的数据资产与处理活动纷繁复杂，且涉及众多的业务场景、业务部门，往往缺乏集

中、全面的盘点。该等盘点是开展自评估与申报的事实基础，建议企业尽快对出境所涉的数据规模、范围、种类、敏感程度、以及处理的目的、范围、方式等情况进行盘点。

2.确定数据出境的合规路径。不同的数据出境活动可能适用不同的合规路径，如安全评估、标准合同、专业认证等。建议企业从自身性质、数据性质、数据量级等角度，依法确定其数据出境活动是否需适用安全评估。

3.开展自评估。自评估是所有数据出境活动均适用的内部机制，但根据不同的合规路径，具体的评估项存在一定差异。建议企业设计、整合自评估的流程与内容，满足不同法律法规对自评估的要求，并切实开展自评估工作、形成可提交监管机构的评估报告。

4.拟定法律文件、落实安全措施。无论适用何种合规路径，数据处理者和境外接收方均需签订具有法律约束力的文件，如合同、单方承诺、有约束力的公司规则等。此外，该等文件并不只是书面条款，更关键的是确保境外接收方具备实质性的安全保护能力，尤其是落实各类管理措施、技术措施。