2022 年 7 月 18 日

企业如何办理数据出境安全评估——《数据出境安全评估办法》正式发布

2021 年 10 月 29 日，国家互联网信息办公室公布了《数据出境安全评估办法（征求意见稿）》，规定了在目前的《个人信息保护法》、《数据安全法》、《网络安全法》体系下企业就数据出境如何进行安全评估手续（以下简称“**安全评估**”）。2022 年 7 月 7 日，《数据出境安全评估办法》（以下简称“**本办法**”）正式发布。本文拟根据正式出台的《数据出境安全评估办法》，整理其与征求意见稿的变动之处，以及梳理目前企业有数据出境需求时应当如何办理相关手续。

一、本办法的修改亮点

根据我们的梳理，正式发布的《数据出境安全评估办法》对此前的征求意见稿做出了一定的修改，我们对修改进行了梳理，具体内容请见附表。与此前的征求意见稿相比，本办法的正式出台文件做了不少修改，主要体现在以下几点：

亮点	相关修改
起算限定	适用安全评估的条件之一“累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息”改为“**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”。
自评估重点	“数据出境和再转移后泄露、毁损、篡改、滥用等的风险”改为“数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险”。
完备性查验	增加了“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”的程序。
出境合同增加了风险防范点	增添了“所在国家、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导致难以保障数据安全”及“出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险”。
取消延长评估时间限制	将“情况复杂或者需要补充材料的，可以适当延长，但一般不超过六十个工作日”改为“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”。
复评程序	增加了“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”。
宽限期	本办法自 2022 年 9 月 1 日起施行，且为企业留出了本办法施行之日起 6 个月内完成整改的宽限期。
出境定义（来自答记者问）	本办法所称数据出境活动主要包括：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。

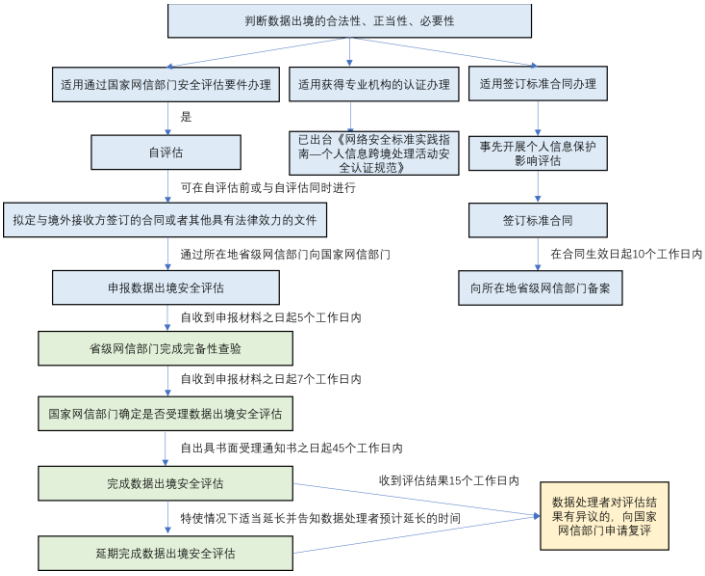
二、企业应当按照何种流程办理安全评估

当企业有数据出境需求时，应当按照下列流程办理手续。

步骤	流程及办理内容
1.	企业应首先判断数据出境是否满足目的、范围、方式等的合法性、正当性、必要性的要求。
2.	如果满足，应当考虑适用《个人信息保护法》下三种要件中的何种要件进行办理。三种要

	件分别为：1）通过国家网信部门安全评估、2）获得专业机构的认证、3）签订国家网信部门制定的标准合同。如果企业属于关键信息基础设施运营者（CIIO）和处理个人信息达到国家网信部门规定数量（于本办法中规定，详见后文）的个人信息处理者，确需向境外提供数据的，应当适用通过国家网信部门组织的安全评估这一要件。
3.	如果属于本办法规定的四种情况（详见后文），企业应当事先进行自评估，并通过所在地省级网信部门向国家网信部门申报安全评估，按照规定提交材料。企业自评估时应当重点评估六个方面（详见后文）。
4.	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。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。
5.	申报材料报送国家网信部门后，国家网信部门应当自收到申报材料之日起 7 个工作日内，确定是否受理并书面通知数据处理者，自向数据处理者发出书面受理通知书之日起 45 个工作日内完成数据出境安全评估，重点评估七个方面（详见后文）。
6.	情况复杂或者需要补充、更正材料的，安全评估可以适当延长并告知数据处理者预计延长的时间。正式发布稿取消了征求意见稿中延长时间一般不超过六十个工作日的限制，复杂情况或者需要补充材料的情况下评估时间可能较长，建议符合条件的企业尽快准备相关材料和手续。

企业办理数据出境安全评估的全流程如下图所示：



三、企业如何判断数据出境是否合法、正当、必要

企业有数据出境需求时，应当首先考虑数据出境的目的、范围、方式等的合法性、正当性、必要性。根据本办法，企业进行数据出境应当满足目的、范围、方式等方面的合法性、正当性、必要性，缺一不可。

在以往的实务中，例如某些企业以提升服务水平等非常模糊的概念为目的向境外母公司提供数据，但境外母公司实际并不参与服务的提供及升级；或者境外母公司只是为了获取境内子公司或孙公司的数据；或者境外母公司仅出于在境外存储或备份这些信息的目的要求境内公司进行跨境传输；我们认为这些情况下数据出境可能将缺乏必要性，无法满足《个人信息保护法》和本办法对数据出境的前提条件要求。

四、企业如何判断是否需要申报安全评估

如前文所述，如属于本办法规定的四种情况，企业应当事先进行自评估，并通过所在地省级网信部门向国家网信部门申报安全评估，按照规定提交材料。这四种情况分别是：

①. 数据处理者向境外提供重要数据；

②. 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；

③. 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；

④. 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。

1. 关于起算时间限定

第三种情况“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”与此前发布的《个人信息出境标准合同规定（征求意见稿）》中的适用条件“（三）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；（四）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”相衔接，便于数据处理者进行判断。同时，设置特定期限也避免了将较长时间内处理数据的企业均纳入安全评估范畴，为动态处理数据的企业提供了便利。

2. 关于国家网信部门规定数量

根据《个人信息保护法》第四十条，如果企业属于关键信息基础设施运营者和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，确需向境外提供数据的，应当通过国家网信部门组织的安全评估，适用本办法办理安全评估。本办法明确了前述规定数量（处理 100 万人以上个人信息、或者自上年 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），为前述第四十条的实施落实提供了标准，同时本办法生效稿进一步明确以具体人数而非个人信息数量为标准。

3. 关于重要数据

关于重要数据，本办法没有规定条数或者容量限制，因此企业只要存在向境外提供重要数据，均应事先申报安全评估。本办法生效稿中增加了对重要数据的定义，是指一旦遭到篡改、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。同时，个别行业出现了以个人信息主体人数达到一定规模来认定重要数据的倾向。比如，《汽车数据安全管理若干规定（试行）》规定，涉及个人信息主体超过 10 万人的个人信息属于重要数据。这种认定方式，将带来个人信息与重要数据的范围出现交叉，值得进一步关注。

4. 关于关键信息基础设施运营者（CIIO）

关键信息基础设施（CII）运营者（CIIO）收集和产生的个人信息和重要数据，属于一种身份要件，即只要具有 CIIO 的身份，其将收集产生的个人信息和重要数据（不论数量及内容）对外提供时，均需要申报进行安全评估。根据 2021 年 9 月 1 日生效的《关键信息基础设施安全保护条例》，CII 的定义是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。该条例规定由行业主管部门、监管部门进一步制定 CII 认定规则，今后应进一步关注认定规则的制定动向。

五、企业申报安全评估应提交哪些材料

企业申报安全评估应当提交以下材料：

①. 申报书；

②. 数据出境风险自评估报告（请详见第六部分）；

③. 数据处理者与境外接收方拟订立的法律文件（请详见第七部分）；

④. 安全评估工作需要的其他材料。

此次发布稿中将数据处理者和境外接收方签订的“合同”修改为“相关合同或者其他具有法律效力的文件等”，将“合同”的范围扩大为“法律文件”。

六、企业如何进行自评估

本办法要求安全评估坚持风险自评估与安全评估相结合。因申报安全评估应当提交的材料中包括数据出境风险自评估报告，因此企业在申报安全评估之前，应当事先进行自评估。自评估是申报安全评估的前置条件。关于自评估，企业可以自行内部开展，也可以在外部专家协助的情况下进行。

需要说明的是，企业自评估中重点评估的六个方面与国家网信部门安全评估中重点评估的七个方面有较多重合之处（详见下表），因此企业在自评估时即应当规范前述问题，为申报安全评估做准备。

序号	自评估的 6 项重点评估事项	安全评估的 7 项重要评估事项
1.	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；	数据出境的目的、范围、方式等的合法性、正当性、必要性；
2.		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；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；
3.	出境数据的规模、范围、种类、敏感程度，数据出境可	出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到

	能对国家安全、公共利益、个人或者组织合法权益带来的风险；	篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；
4.	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数据的安全；	数据安全和个人信息权益是否能够得到充分有效保障；
5.	数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；	
6.	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等（以下统称法律文件）是否充分约定了数据安全保护责任义务；	数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；
7.		遵守中国法律、行政法规、部门规章情况；
8.	其他可能影响数据出境安全的事项。	国家网信部门认为需要评估的其他事项。

其中，前述国家网信部门安全评估中重点评估的七个方面包含“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；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求”，因此还可能涉及对境外接收方所在国家或者地区的数据保护水平的评估，企业应当重点关注境外接收方所在国家或地区、境外接收方自身的数据保护水平等技术方面的要求。

七、企业如何与境外接收方签订合同等法律文件

因申报安全评估应当提交的材料中，包括数据处理者与境外接收方拟订立的法律文件，因此企业在申报安全评估之前，应当至少拟定与境外接收方签订的法律文件。本办法要求企业应当明确与境外接收方约定数据安全保护责任义务，且至少将以下内容涵盖在合同内：

①. 数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

②. 数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

③. 对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

④. 境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、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导致难以保障数据安全时，应当采取的安全措施；

⑤. 违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

⑥. 出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

结语

《数据出境安全评估办法》的正式生效，为企业就数据出境办理安全评估提供了实施路径，也意味着数据出境安全评估正式落地，开启了安全评估手续办理通道。对于符合本办法中四种应申报安全评估的情况且确有数据出境需求的企业，应当尽早梳理数据出境情况，委托专业机构或自行进行自评估，与境外接受方签订符合要求的数据出境合同等法律文件，尽早进行安全评估申报。本办法虽给予了六个月宽限期，但考虑到首先要做自评估，做自评估时首先需要进行数据处理情况摸底，发现问题后及时整改，为顺利通过安全评估通常需要提交整改完成后的自评估报告，考虑到自评估、整改、修改自评估报告均需花费较多时间进行处理，建议符合条件的企业尽快开展相关工作，积极调整数据出境业务框架，确保在合规的前提下开展业务。

本办法发布稿与《征求意见稿》主要修改点对比附表：

序号	**《数据出境安全评估办法（征求意见稿）》**	**《数据出境安全评估办法》**
1.	第四条 数据处理者向境外提供数据，符合以下情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。 （一）关键信息基础	第四条 数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估： （一）**数据处理者向**

	设施的运营者收集和产生的个人信息和重要数据； （二）出境数据中包含重要数据； （三）处理个人信息达到一百万人的个人信息处理者向境外提供个人信息； （四）累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息； （五）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。	**境外提供重要数据**； （二）**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； （三）**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； （四）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。
2.	第五条 数据处理者**在向境外提供数据前**，应~~事先~~开展数据出境风险自评估，重点评估以下事项： （一）数据出境及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； （二）出境数据的**数量、**范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险； ~~（三）数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险；~~ （四）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数据的安全； （五）数据**出境和再转移后泄露、毁损、篡改、滥用等**的风险，个人维护个人信息权益	第五条 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，重点评估以下事项： （一）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； （二）出境数据的**规模**、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险； （三）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数据的安全； （四）数据**出境中和出境后**遭到**篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等**的风险，个人信息权益维护的渠道是否通畅等； （五）与境外接收方拟订立的数据出境**相**
	的渠道是否通畅等； （六）与境外接收方订立的数据出境**相关合同**是否充分约定了数据安全保护责任义务。	**关合同或者其他具有法律效力的文件等（以下统称法律文件）**是否充分约定了数据安全保护责任义务； **（六）其他可能影响数据出境安全的事项。**
3.	第七条 国家网信部门自收到申报材料之日起七个工作日内，确定是否受理评估并以书面通知形式反馈受理结果。	第七条 **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。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。** 国家网信部门应当自收到申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者。
4.	第九条 数据处理者与境外接收方订立的合同**充分**约定数据安全保护责任义务，**应当包括但不限于**以下内容： （二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者**合同**终止后出境数据的处理措施； （三）**限制**境外接收方将出境数据再转移给其他组织、个人的**约束条款**； （四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区**法律环境发生变化**导致难以保障数据安全时，应当采取的安全措施；	第九条 数据处理者**应当**在与境外接收方订立的法律文件中**明确**约定数据安全保护责任义务，**至少包括**以下内容： （二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者**法律文件**终止后出境数据的处理措施； （三）**对于**境外接收方将出境数据再转移给其他组织、个人的**约束性要求**； （四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、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**导致

	（五）违反数据安全保护义务的**违约责任和具有约束力且可执行的争议解决条款**； （六）**发生数据泄露等风险时**，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。	难以保障数据安全时，应当采取的安全措施； （五）违反法律文件约定的数据安全保护义务的**补救措施、违约责任和争议解决方式**； （六）**出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时**，妥善开展应急处置的要求和保障个人维护其个人信息权益的**途径和方式**。
5.	第十条 国家网信部门受理申报后，组织~~行业主管部门~~、国务院有关部门、省级网信部门、专门机构等进行安全评估。 ~~涉及重要数据出境的，国家网信部门征求相关行业主管部门意见。~~	第十条 国家网信部门受理申报后，**根据申报情况**组织国务院有关部门、省级网信部门、专门机构等进行安全评估。
6.	第十三条 **数据处理者应当按照本办法的规定提交评估材料，材料不齐全或者不符合要求的，应当及时补充或者更正，拒不**补充或者更正的，国家网信部门可以终止安全评估；数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理。	第十一条 **安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正**。数据处理者**无正当理由**不补充或者更正的，国家网信部门可以终止安全评估。 数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，**并依法追究相应法律责任**。
7.	第十一条 国家网信部门自出具书面受理通知书之日起四十五个工作日内完成数据出境安全评估；**情况复杂或者需要补充材料的，可以适当延长，但一般不超过六十个工作日。**	第十二条 国家网信部门应当自向数据处理者发出书面受理通知书之日起45个工作日内完成数据出境安全评估；**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。**
8.	/	第十三条 **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。**
9.	第十二条 **数据出境评估结果有效期二年**。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：（二）境外接收方所在国家或者地区**法律环境**发生变化，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**合同**变更等可能影响出境数据安全的； ~~未按本条规定重新申报评估的，应当停止数据出境活动。~~	第十四条 **通过数据出境安全评估的结果有效期为2年**，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：（二）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；
10.	第十四条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。	第十五条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供、**非法使用**。
11.	第十五条 任何组织和个人发现数据处理者**未按照**本办法规定**进行评估向境外提供数据的**，可以向省级以上网信部门投诉、举报。	第十六条 任何组织和个人发现数据处理者**违反**本办法**向境外提供数据的**，可以向省级以上网信部门举报。
12.	第十六条 国家网信	第十七条 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，应当**撤销评估结果并书面通知数据处理者，数据处理者应当终止数据出境活动**。需要继续开展数据出境活动的，数据处理者应当按照要求进行整改，并在整改完成后重新申报评估。	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，应当**书面通知数据处理者终止数据出境活动**。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。
13.	/	第十九条 本办法所称重要数据，是指一旦遭到篡改、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。
14.	第十八条 本办法自 年 月 日起施行。	第二十条 **本办法自2022年9月1日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起6个月内完成整改。**

杨锦文 合伙人 电话：86 10 8553 7608 邮箱地址：yangjw@junhe.com

李圆圆 律 师 电话：86 10 8540 8665 邮箱地址：liyuanyuan@junhe.com