

一文明辨数据出境安全评估

作者：潘永建 | 沙莎

2022 年 9 月 1 日,《数据出境安全评估办法》(“《评估办法》”)生效,正式确立网信部门主导的数据出境安全评估要求和门槛。根据《评估办法》,数据出境安全评估应当“坚持事前评估和持续监督相结合、风险自评估与安全评估相结合”的原则,即在数据出境安全评估的基础上设置“自评估”的前置要求。按照《个人信息保护法》,另一前置要求是进行个人信息保护影响评估。

除上述规定之外,此前多部法律法规征求意见稿亦对企业个人信息和重要数据出境行为提出评估要求,包括 2019 年 6 月颁布的《个人信息出境安全评估办法》¹以及 2017 年 4 月颁布的《个人信息和重要数据出境安全评估办法》。

事前评估、数据出境安全评估、数据出境风险自评估、个人信息保护影响评估、个人信息出境安全评估.....面对各类评估要求,企业或感雾里看花,对于应当在哪个阶段参照何种规定完成评估要求有所疑虑。本文通过对数据出境法规的梳理,帮助企业明辨数据出境评估要求,为数据跨境传输合规提供行之有效的方法论。

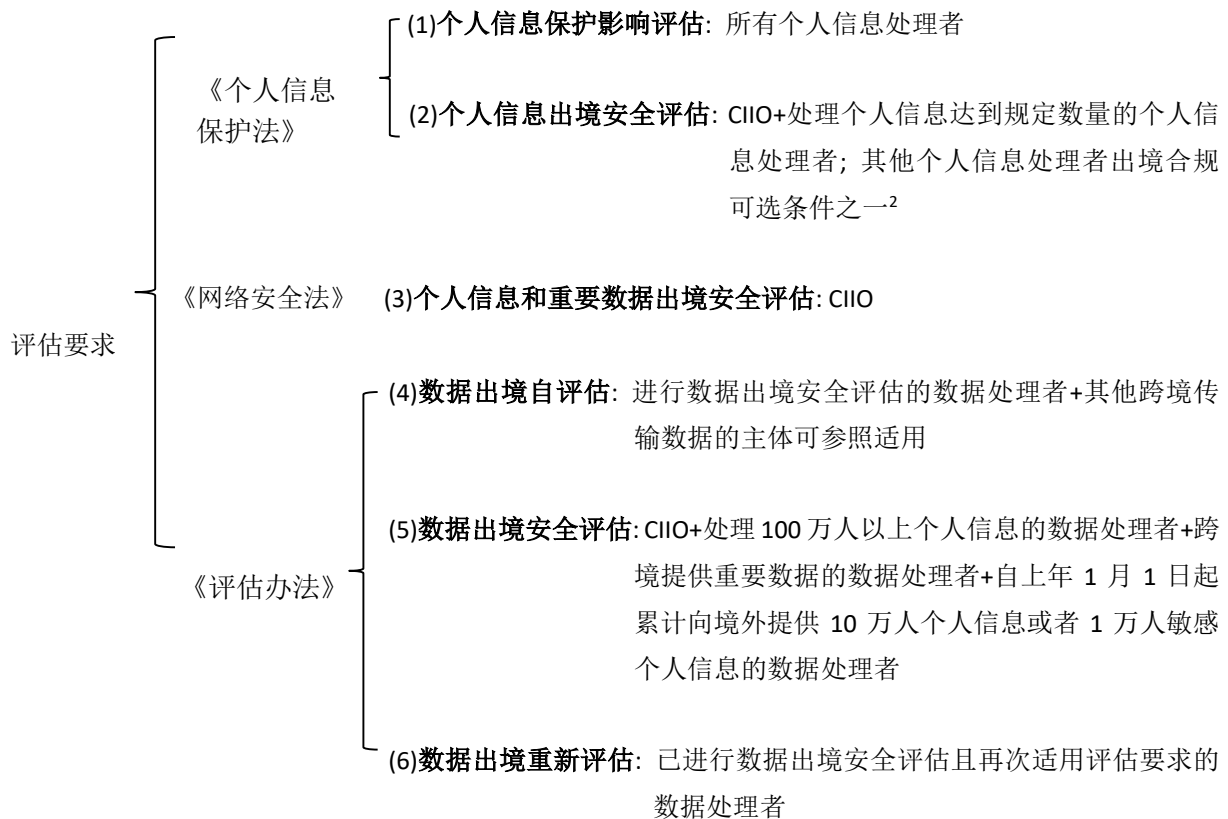
一. 评估类型

从生效法律法规来看,《个人信息保护法》《网络安全法》和《评估办法》分别提出了数据出境评估要求。

.....
如您需要了解我们的出版物,
请联系:

Publication@linksllaw.com

¹ 《个人信息出境安全评估办法》第一版征求意见稿于 2017 年 4 月 11 日颁布。



除生效法规外,《个人信息出境安全评估办法(征求意见稿)》规定的“网络运营者”向境外提供个人信息需要向省级网信部门申请安全评估,以及《个人信息和重要数据出境安全评估办法(征求意见稿)》规定的“网络运营者”向境外提供个人信息和重要数据需要向行业主管或监管部门申报评估的要求,实际已经被《评估办法》的规定所取代,企业按照《评估办法》规定的门槛和要求申报评估即可。

尽管《网络安全法》《个人信息保护法》以及《评估办法》规定的的数据出境相关的评估类型繁多,适用主体的表述也各不相同,但结合数据出境评估各项规定,就当前生效法律法规,企业在数据出境过程中应进行个人信息保护影响评估、数据出境风险自评估和数据出境安全评估三类评估。

二. 个人信息保护影响评估

对于跨境传输个人信息的企业而言,无论跨境传输个人信息的数量或所涉个人信息主体的数量如何,在跨境传输个人信息前,均应当进行个人信息保护影响评估。根据《个人信息保护法》的要求,个人信息保护影响评估应当包括以下三项内容:

- (1) 评估个人信息的处理目的、处理方式等是否合法、正当、必要;
- (2) 评估个人信息出境行为对个人权益的影响及安全风险;
- (3) 评估为跨境传输个人信息所采取的保护措施是否合法、有效以及是否与风险程度相适应。

² 尽管《个人信息保护法》规定“通过国家网信部门组织的安全评估”是个人信息处理者可选择的四项基本条件之一,但未达《评估办法》规定门槛的企业申报评估,网信部门是否受理有待实践证实。

此外,2022年7月公布的《个人信息出境标准合同规定(征求意见稿)》对跨境传输个人信息场景下的个人信息保护影响评估的内容进行了进一步细化补充,评估内容包括:

- (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。

个人信息保护影响评估的概念类似于欧盟法下的 DPIA(Data Protection Impact Assessment),该等评估重点关注个人信息处理场景中的高风险处理行为,要求个人信息处理者从个人信息处理目的、方式、风险、对个人的影响和保护措施等维度评估数据处理行为的风险等级,并确定需要采取的降低风险的措施。

通常情况下,个人信息保护影响评估是企业处理个人信息时必须搭建的合规框架,个人信息跨境传输场景仅为个人信息保护影响评估的评估事项之一。在《个人信息保护法》生效前,部分企业,特别是跨国公司可能已经针对个人信息处理行为进行过类似评估,该企业则可在过往个人信息保护影响评估的基础上按照《个人信息保护法》的要求进行调整和更新。

三. 自评估

根据《评估办法》的要求,数据出境风险自评估是数据出境安全评估的前置步骤,企业在申报数据安全评估时,数据出境风险自评估报告也是必须提交的材料之一。对于达到数据出境安全评估门槛的企业而言(大概率需要进行个人信息保护影响评估),可以在个人信息保护影响评估的基础上,增加自评估的相关内容,以此节约合规成本。

数据出境风险自评估报告主要有两部分内容,一是对数据出境活动整体情况的描述,自评估报告中应当写明:

1. 出境方:数据处理者的基本情况+安全保障能力的描述
2. 业务和系统:数据出境涉及业务和系统的情况
3. 出境数据:拟出境数据的情况
4. 境外接收方:境外接收方的情况,包括基本情况、处理数据的用途、方式、数据安全保障能力、所在国家/地区的数据保护环境等
5. 法律文件:数据出境法律文件约定的数据安全保护责任义务

对数据出境活动的整体情况进行描述后,自评估报告中还需根据基本情况对出境数据的风险进行评估,评估维度应当涵盖《评估办法》规定的六类重点评估事项。

四. 安全评估

我们在此前的[《尘埃落定!一文详解<数据跨境传输安全评估>重点规定》](#)[《双语图解!一图读懂数据出境安全评估及申报规则》](#)等文章中,已经对数据出境安全评估申报与审查适用情形、流程、要求进行了详细解读。

在申报数据出境安全评估时,应当按照《数据出境安全评估申报表》的要求对数据出境业务、目的、方式、链路情况、拟出境数据的情况、境外接收方的情况进行描述,同时一并提交《数据出境风险自评估报告》,由网信部门最终判断数据出境风险的高低,并据此作出评估结果。

总结而言,就个人信息保护影响评估、数据出境风险自评估和数据出境安全评估的适用:

1. 凡涉及个人信息出境的企业,必须进行个人信息保护影响评估;
2. 达到数据出境安全评估门槛的企业,需首先进行数据出境风险自评估,自评估可在个人信息保护影响评估的基础上进行,主要内容应当包括数据出境活动的整体概述和对数据出境活动风险的评估;
3. 完成数据出境风险自评估后,应当在3个月内申报数据出境安全评估。如果截至申报日,数据出境情况发生重大变化³,企业应当重新进行自评估后才可申报数据出境安全评估。

申报数据出境安全评估后,如果数据出境安全评估有效期届满(自结果出具之日起2年)且企业仍继续跨境传输数据,或者在有效期内数据出境情况发生重大变化,则申报企业应当重新申报评估。

五. 其他评估

需要注意的是,在非出境场景下,企业仍可能需要履行网络数据安全评估义务。

对于个人信息处理者而言,除出境场景外,企业还需就处理敏感个人信息、委托个人信息、共享个人信息等场景开展个人信息保护影响评估。

对于重要数据处理者而言,企业应当就重要数据的处理情况定期开展风险评估并报送主管部门。目前《汽车数据安全若干规定(试行)》已对汽车重要数据的内涵进行界定,并要求处理汽车重要数据的处理者向有关部门报送风险评估报告。

对于构成关键信息基础设施运营者的企业而言,需要按照《网络安全法》以及《关键信息基础设施安全保护条例》等法律法规的要求,对关键信息基础设施每年至少进行一次网络安全检测和风险评估,对发现的安全问题及时整改,并按照保护工作部门要求报送情况。

³ 参照《评估办法》的规定,重大变化一般包括:(1)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;(2)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;(3)出现影响出境数据安全的其他情形。

如您希望就相关问题进一步交流, 请联系:



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求, 请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明:

本出版物仅供一般性参考, 并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2022