“个人信息保护影响评估”的合规与实践

作者：杨迅 | 象玉婷

2021 年 11 月 1 日正式生效的《个人信息保护法》是我国第一部在个人信息保护领域的综合性立法，它明确提出了个人信息处理者开展个人信息保护影响评估的要求。据此，企业如何开展个人信息保护影响评估，成为继 APP 合规之后的另一个个人信息保护合规要点。

一. 个人信息保护影响评估概况

开展个人信息保护影响评估不仅是个人信息处理者的法定义务，也是其控制个人信息安全风险的重要保障。制定相应的制度开展个人信息影响评估，既能够帮助企业更好的落实个人信息保护合规义务，又能规范企业的个人信息处理活动。

(一) 个人信息保护影响评估及其法律框架体系

个人信息保护影响评估是针对个人信息处理活动，检查其合法合规性，判断其对个人合法权益造成的影响，以及评估个人信息保护措施有效性的过程。

在法律法规层面，《个人信息保护法》第 55 条(“**《个保法》**”)明确规定了个人信息处理者在处理敏感个人信息，进行自动化决策，委托处理、对外提供、公开个人信息以及向境外提供个人信息时，需要事前进行个人信息保护影响评估并对处理情况进行记录的法定要求；《数据安全法》中规定了重要数据的处理者对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告的义务；《个人信息出境安全评估办法(征求意见稿)》规定了网络运营者在向境外提供在中国境内运营中收集的个人信息时，应当进行安全评估，并进一步规定了评估的方式和内容等。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

在国家标准层面，《信息安全技术 个人信息安全规范》以及《信息安全技术 个人信息安全影响评估指南》对个人信息安全影响评估的定义、原理、场景和框架、评估流程、评估的具体实施方式进行了详细的说明；《信息安全技术 数据出境安全评估指南(征求意见稿)》则对个人信息及数据出境的安全评估流程、要点和方法进行说明。

(二) 企业开展个人信息保护影响评估的意义

开展个人信息保护影响评估，对企业而言具有以下意义:

(1) 如前文所述，开展个人信息保护影响评估是《个保法》下的法定义务;
(2) 开展个人信息保护影响评估可以通过识别个人信息处理行为与法律、法规、标准或良好的行业实践之间的差距，并据此采取适当的安全控制措施;
(3) 开展个人信息保护影响评估形成的记录文档在发生个人信息安全事件时，可以在监管机构调查、执法、合规审计等法律程序中，作为企业证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的证据;
(4) 个人信息保护影响评估有利于持续关注法律监管环境的动态并不断发现、处置和监控个人信息处理过程对个人信息主体合法权益的影响和潜在风险，建立企业个人信息保护的公信力，以进一步改进和提升自身的安全风险管理能力，实现“动态合规”。

二. 个人信息保护影响评估的适用场景

(一) 法定评估场景

《个保法》和其他法律规范规定了必须开展个人信息保护影响评估的场景。

从行为角度，《个保法》第 55 条规定: 处理敏感个人信息，进行自动化决策，委托处理、对外提供、公开个人信息以及向境外提供个人信息时，开展个人信息影响评估是个人信息处理者的法定义务，否则未履行法定义务将可能面临严厉的法律责任及相关监管机关的处罚。

从时间节点看，《信息安全技术 个人信息安全规范》第 11.4 节中规定了必须要进行个人信息安全影响评估的情形，比如当产品或服务发布前或业务功能发生重大变化时，发生重大个人信息安全事件，在法律法规有新要求或业务模式、信息系统、运行环境发生重大变更时等情形时，均需要开展个人信息安全影响评估。

结合以上两个角度,当企业涉及处理敏感个人信息，进行自动化决策，委托处理、对外提供、公开个人信息或向境外提供个人信息时，以及产品、服务或业务开展前、发生重大变化时或者其技术、法律环境发生重大变化时，需要开展个人信息保护影响评估。

(二) 尽责性评估场景

在符合相关法律、法规和标准的基线要求之上，出于审慎经营、声誉维护、品牌建立等目的，企业还可以选取可能对个人合法权益产生高风险的个人信息处理活动，开展尽责性风险评估，以降低对个人信息主体合法权益的不利影响。

《信息安全技术 个人信息安全影响评估指南》附录中列举了高风险的个人信息处理活动示例，比如银行在提供贷款前使用人工智能算法对个人信息主体进行信用评估，数据处理可能涉及与信用评估没有直接关联的个人信息；又如电商平台监控用户购物行为，进行用户画像，分析用户的购买偏好和购买能力；再如医疗大健康企业通过智能手表、手环或其他移动设备持续收集和监控个人信息主体的活动、健康相关数据等。除此之外，在中国的法制环境和制度语境下，一般影响波及的人群范围广，对公共利益有较大影响的个人信息处理场景，被认定为高风险的个人信息处理活动的概率较高，比如系统性的监控分析个人或个人信息、在公共区域监控、采集个人信息等场景。

三. 个人信息保护影响评估的基本流程

(一) 法律及相关国标的要求

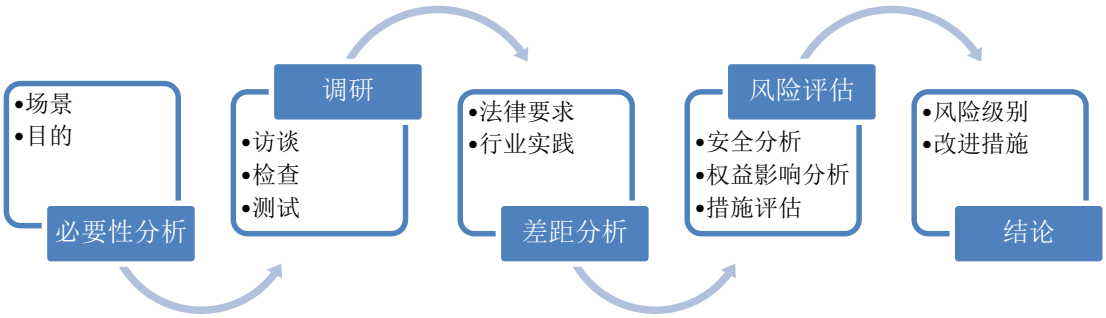
根据《个保法》第 56 条的规定，个人信息保护影响评估应当包括下列内容: (1)个人信息的处理目的、处理方式等是否合法、正当、必要; (2)对个人权益的影响及安全风险; (3)所采取的保护措施是否合法、有效并与风险程度相适应；除此之外，《个人信息安全影响评估指南》、《个人信息安全规范》以及《数据出境安全评估指南(征求意见稿)》中也对评估的内容、流程及方式进行了规定，对企业开展个人信息保护评估提供了重要的参考。

(二) 评估责任主体

通常而言，企业开展个人信息保护影响评估工作可以由其法务部门、合规部门或其信息安全部门牵头执行。上述责任部门或人员在开展评估时应当具有独立性，在不受被评估方影响的前提下，负责工作流程制定、实施和改进，并对个人信息保护影响评估的质量负责。上述企业内部的责任部门可以根据部门的具体能力配备情况，自行开展个人信息保护影响评估工作，或聘请外部独立的第三方来承担具体的评估工作。

(三) 个人信息保护影响评估的基本流程

企业进行个人信息保护影响评估的基本目标是为了调研和分析企业特定产品或服务所涉及的个人信息处理活动的合法性、正当性、必要性，并对处理活动的中风险源以及对个人权益的影响及其程度进行识别和评估，通过综合两方面的结果得出个人信息处理活动的风险等级，并据此提出相应的改进措施。具体而言，可以按照以下步骤进行:



(1) 必要性分析

个人信息保护影响评估的必要性分析，取决于企业开展个人信息保护影响评估的场景和自身的个人信息安全目标。企业可以根据实际的需求选取需要启动评估的业务场景，例如：产品或服务的年度整体评估；新产品或新服务的上线初次评估；行业法律法规、政策、标准或业务模式、互联网安全环境等外部环境发生重大变化时重新评估等，并锁定特定的评估目标，比如特定的合法合规要求或者满足较高的个人信息保护水平等。

(2) 调研方式

进行个人信息保护影响评估的调研方式，包括但不限于以下三种：**(a)访谈**，即通过访谈的方式对个人信息的处理、保护措施和实施情况进行了解、分析和取证，访谈的对象可以包括涉及个人信息处理各环节的产品经理、研发工程师、安全管理人员、运维人员等；**(b)检查**，即通过对管理制度、合作协议、安全策略等进行观察查验，比如对个人信息保护制度、系统设计文档和接口规范、应急演练结果等进行检查；**(c)测试**，即通过人工或自动化安全测试工具进行技术测试，比如对访问控制、身份识别验证、保存加密机制等进行测试。企业通过上述方式对个人信息的处理场景进行深度的调研。

(3) 差距分析

在进行差距分析时，企业可以根据所适用的个人信息保护相关法律、法规、政策及相关国标、行业标准等分析自身的个人信息处理活动与上述适用规则的差距，还可以参考借鉴同行业对类似场景的处理方式和实践进行分析。《个人信息安全影响评估指南》附录 C 中表 C1《基于处理活动/场景/特征或组件的个人信息映射表》和 C2《个人信息生命周期安全管理》可以为企业进行差距分析提供参考。

(4) 风险识别和评估

在风险识别和评估环节，企业需要首先对特定的个人信息处理活动中的风险源进行识别，分析是否缺乏足够的安全措施，导致存在脆弱性而引发安全事件的可能性。其中，就威胁

源而言，既有内部的威胁源(如：内部人员操作不当导致数据泄露)，又有外部的威胁源(如：被第三方恶意窃取)；就防御缺陷导致的脆弱性而言，既有物理环境缺陷导致的(如：储存环境不当)，也有技术因素或管理不当造成的数据泄露、篡改、丢失、滥用等事件。

通过识别的风险，进一步考察：(1)所述风险对个人权益的可能危害，包括限制个人自主决策权、引发差别待遇、名誉受损或精神压力以及人身财产损害；(2)该些危害发生的可能性。根据上述因素，综合评估风险的高低。

(5) 结论和改进措施

根据风险评估的结果，企业可以根据风险高低和风险控制的可能性实施相应的安全控制措施进行风险处置，采取立即处置、限期处置、权衡影响和成本后处置、接受风险等处置方式，并持续跟踪风险处置的落实情况。

四. 常见问题及建议

实践中，对于不少企业来说，涉及个人信息处理活动的业务复杂多变，第三方供应商、合作伙伴众多，会频繁的触发需要进行个人信息保护影响评估的场景，那么如何简化高频、繁琐的评估流程适应企业的具体情况，又能满足法律合规义务呢？

这就需要对个人信息影响评估的场景开展模块化的梳理，建立“白名单/红名单”，以及以变量为导向的评估流程。

首先，我们建议企业根据自身业务的特点和内部风险管理政策，自行或委托外部的专业组织，对日常业务中典型的、具有共性的个人信息处理模式进行分类梳理，确定需要评估的主要元素和标准，并以此建立个人信息保护影响评估表，从而简化和规范化评估流程，作为大部分个人信息处理场景评定的依据。

其次，企业可以对日常个人信息出境的场景开展预评估，确立白名单。对于日常经营活动中的，需要个人信息保护影响评估的处理行为，可以就共同的因素作出评估，风险较低的，纳入白名单，之后落入白名单范围的个人信息处理行为则不需要另行评估。

同时，在日常或对可能涉及的“变量”，比如个人信息的数量、敏感程度、处理的频率、用户的规模、系统安全环境以及第三方供应商、合作伙伴的信用等设置一个“阈值”或“变量”。对于落入预先设定的“阈值”范围的，可以按照预先设定的评估表和白名单进行风险判定，并根据判定结果采取相应的保护或改进措施；对于超过预先设定的“阈值”，但在可变量范围内的，可以根据变量的处理规则判定，比如增加更多、更强的保护措施。

最后，对于超出预先设定的“阈值”，或者根据评估认为可能对个人合法权益产生高风险的个人信息处理活动，纳入红名单中，并在触发相关场景时自行或通过外部机构进行评估和风险预警，以采取合理有效的预防或修正措施，降低对个人信息主体合法权益的不利影响，规范企业的个人信息处理行为。

举例而言，比如对业务涉及个人信息跨境传输的跨国企业而言，若其向同一境外的接受者多次或连续的提供种类相同的个人信息时，那么企业可以根据预先设定的评估表对跨境传输的个人信息处理活动进行常规性的评估；若接收者不同或出境的个人信息种类或数量发生了质的变化，则需要根据这些“变量”对安全事件发生可能性及个人权益影响的程度进行专门的判定，在原有常规判定表的基础上，增加针对性的风险分析及改进措施或根据具体情况另行制作评估报告。

又如，对于涉及第三方供应商、商业合作伙伴众多的企业而言，可能需要经常涉及对外提供或委托上述第三方处理个人信息的场景，企业可以通过调查(公开的查询、安全事件的调查等)对相关第三方的安全保护措施、能力和水平以及所处国家或地区的网络安全环境等对第三方进行“白名单/红名单”的分类，对于综合个人信息保护水平较高、合作多次且未发生过安全事件的第三方可以归入白名单，进行评估时可以根据预先设定的评估表进行分析评估，而对于落入红名单的合作方则可能需要专门评估其个人信息的安全保护措施、能力和水平等，并在合作过程中加强对其的监督和审查，以约束其个人信息处理行为。

如您希望就相关问题进一步交流，请联系:

杨 迅
+86 21 3135 8799
xun.yang@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	北京	深圳
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	伦敦	
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	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