2020 年 12 月 28 日

山顶千门次第开—企业如何落实《个人信息安全影响评估指南》

随着中国踏步跨入大数据时代，个人信息保护的重要性日益凸显，从2017年《网络安全法》开始，个人信息安全相关法规及国家标准相继公布、实施，呈现“山顶千门次第开”的景象。作为其中的重要门户，2020年11月19日，国家市场监督管理总局、国家标准化管理委员会正式发布了《信息安全技术 个人信息安全影响评估指南》GB/T39335-2020国家标准（以下简称“**《评估指南》**”），并将于2021年6月1日正式实施。

《评估指南》为相关法律和国家标准的实施提供了有效的工具和抓手，也对企业的个人信息保护工作提出了新的要求。企业作为个人信息控制者和处理者，应当如何落实这项要求？本文拟梳理有关个人信息安全影响评估的相关规则，以期为企业的最新合规实务提供参考。

一、个人信息安全影响评估概况

（一）什么是个人信息安全影响评估

“个人信息安全影响评估”（personal information security impact assessment，简称“**PISIA**”），在《网络安全法》、《个人信息保护法（草案）》以及《数据安全法（草案）》中属于“风险评估”或者“安全评估”的范畴[1]。根据《评估指南》，“个人信息安全影响评估”是指针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。个人信息安全影响评估旨在发现、处置和持续监控个人信息处理过程中对个人信息主体合法权益造成不利影响的风险。

（二）安全评估立法的国际动向

2011年以来，国际标准化组织、国际电工委员会先后公布的ISO/IEC 29100：2011《信息技术 安全技术 隐私框架》、ISO/IEC 29134：2017《隐私影响评估》形成了隐私保护标准体系，对隐私影响评估（Privacy Impact Assessment，PIA）的评估过程、评估报告的结构和内容等做了规定。

在欧盟，《一般数据保护条例》（简称“**GDPR**”）专门规定了数据保护影响评估（简称“**DPIA**”）制度。GDPR第35条规定，数据控制者在进行数据处理之前，基于数据处理的性质、范围、内容及目的判断处理活动可能对个人的权利和自由构成高风险时，应实施DPIA[2]。

在日本，隐私影响评估主要体现为“特定个人信息保护评估”制度。根据2013年公布的《关于在行政程序使用识别特定个人的号码等的法律》，以及此后2014年、2018年先后公布的《关于特定个人信息保护评估的规则》、《特定个人信息保护评估指针》等配套规则，日本的行政机关、公共团体等在持有或者拟持有特定个人信息文件时，应预测对个人隐私等的权利利益可能产生的影响，并分析导致产生

[1] 《网络安全法》第 37 条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。
《数据安全法（草案）征求意见稿》第 28 条： 重要数据的处理者应当按照规定对其数据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。
风险评估报告应当包括本组织掌握的重要数据的种类、数量,收集、存储、加工、使用数据的情况,面临的数据安全风险及其应对措施等。
《个人信息保护法（草案）》第 54 条： 个人信息处理者应当对下列个人信息处理活动在事前进行风险评估，并对处理情况进行记录。

[2] 参见中国人民大学丁晓东副教授翻译《一般数据保护条例》。

特定个人信息泄露以及其他事态的风险，通过特定个人信息保护评估表的形式确认并宣布采取减轻该风险的妥当措施[3]。

（三）我国有关PISIA的法规体系及《评估指南》的定位

随着2017年《网络安全法》、《民法总则》的实施，我国不断从民事权利、网络安全的角度强化对个人信息的保护规制，以下图所示的主要体系为中心不断完善。同时，在法律法规、国家标准等不同层面，逐步对个人信息安全影响评估提出明确的要求。

法律层面，2017年实施的《网络安全法》中明确规定了个人信息跨境传输及网络安全事件发生后的安全评估机制，2019年实施的《儿童个人信息网络保护规定》明确规定了企业在儿童个人信息转移及委托处理场景下的安全评估责任。2020年公布的《数据安全法（草案）》规定了重要数据处理者应当定期开展风险评估并向主管部门报送风险评估报告。2020年10月21日最新公布的《个人信息保护法（草案）》，进一步细化了《网络安全法》的有关要求，第54条还专门列举规定了PISIA的适用场景、评估内容及报告形式要件等。

国家标准层面，2018年开始实施的《个人信息安全规范》（2020年10月1日起被GB/T 35273—2020替代）对PISIA做出定义，并详细规定其适用场景，具体包括基于个人信息的自动化决策、个人信息委托处理、共享/转让、公开披露活动等。2018年公布的《信息安全技术 个人信息安全影响评估指南（征求意见稿）》对评估做了统一全面的规定；2019年公布的《个人信息出境安全评估办法(2019征求意见稿)》专门针对个人信息出境，规定了实施评估的场景、主管部门、评估报告内容等。

根据《评估指南》征求意见稿编制说明，《评估指南》是《个人信息安全规范》标准落地的有力抓手，是完善我国个人信息安全保护标准体系的关键环节，使我国首次有了较为权威的评估个人信息安全的方法论与路线图。《评估指南》以标准形式给予个人信息安全保护更科学、更专业、一致性的指导，促进个人信息安全风险评估取得实效，便于监管机构用于检查和监督《个人信息安全规范》的落地，从而支撑《网络安全法》、《个人信息保护法（草案）》以及GDPR项下的DPIA实施工作。

二、个人信息安全影响评估的义务主体及实施形式

（一）义务主体

关于有义务实施个人信息安全影响评估的主体，《个人信息安全规范》规定为 “个人信息控制者”[4]，而《个人信息保护法（草案）》规定为“个人信息处理者”[5]。从用语表达来看，似乎两个规范性文件规定的义务主体互不相同，但是从用语指代的实际内容来看，义务主体的内涵相同，均是指能够自主决定（有能力决定）个人信息处理目的、方式等个人信息处理事项的组织或个人。结合该定义，“能够自主决定个人信息处理目的、方式的组织”范围非常广泛，可能涵盖企业、公司、外国公司驻华机构等，不论通过网络方式或者线下方式自主处理个人信息，只要其处理个人信息的活动落入上述法规、国家标准规定的应当实施评估的情形，均有义务实施个人信息安全影响评估。

（二）评估实施形式

从评估的发起主体来看，个人信息安全影响评估分为自评估和检查评估两种形式。自评估指的是企业等组织自行发起对其个人信息处理行为的评估，检查评估是指企业等组织的上级组织发起的个人信息安全影响评估工作。

从评估的实施主体来看，不论是自评估还是检查评估，都可以指定企业内部专门负责评估、审计

[3] 参见日本个人信息保护委员会 2018 年公布的《特定個人情報保護評価指針の解説》。

[4] 《个人信息安全规范》第 3.4 条：个人信息控制者是指，有能力决定个人信息处理目的、方式等的组织或个人。

[5] 《个人信息保护法（草案）》第 69 条：个人信息处理者，是指自主决定处理目的、处理方式等个人信息处理事项的组织、个人。

的内部岗位或角色（例如法务部门、合规部门或信息安全部门）开展评估；也可以委托外部专业机构（网络安全评估机构、律师等）开展评估工作。值得注意的是，企业指定内部责任部门（一般为上述法务部门、合规部门或信息安全部门）实施评估时，应当保证该部门或责任人员的独立性，防止受到被评估方的影响。根据我们的经验，企业通常会聘请律师等外部专业机构、独立第三方参与评估工作，以保证责任部门在实施评估工作过程的独立性和客观性。

三、基线合规要求——应事先实施安全评估的场景及评估要点

根据《个人信息保护法（草案）》第54条，企业实施以下活动时，需要事先进行风险评估并制作风险评估报告，并记录个人信息处理情况。风险评估报告和处理情况记录应当至少保存三年：

(1) 处理敏感个人信息；

(2) 利用个人信息进行自动化决策；

(3) 委托处理个人信息、向第三方提供个人信息、公开个人信息；

(4) 向境外提供个人信息；

(5) 其他对个人有重大影响的个人信息处理活动。

需要注意的是，全国人大常委会法工委于2020年12月11日举办答记者会，指出2021年度的立法工作计划已纳入对《个人信息保护法》等法律案的继续审议，争取早日出台。根据人大常委会的立法进程，一般认为《个人信息保护法》有望2021年内通过，届时企业在实施第54条规定的个人信息活动之前，将承担实施个人信息安全影响评估的法定义务。

同时，尽管没有列入上述《个人信息保护法（草案）》第54条的规定，但根据《个人信息安全规范》，企业出现以下场景时，为降低个人信息处理活动的违规风险，应开展个人信息安全影响评估：（1）在产品或服务发布前，或业务功能发生重大变化时；（2）在法律法规有新的要求时：（3）在业务模式、信息系统、运行环境发生重大变更时；（4）发生或重大个人信息安全事件时。

对于企业实施上述个人信息处理活动、场景时的安全评估要点，《评估指南》附录A的相关指南做了详细规定，企业可以相应参照实施。

四、主动进取——尽责性风险评估

企业在日常经营过程中，除为遵守相关法规的基线要求而实施安全评估之外，有时出于审慎经营、声誉维护、品牌建立等目的，往往主动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，以尽可能降低对个人信息主体合法权益的不利影响。以下基于《评估指南》附录B，概括常见的高风险个人信息处理活动及场景示例。

个人信息处理活动	场景示例
a）数据处理涉及对个人信息主体的评价或评分，特别是对个人信息主体的工作表现、经济状况、健康状况、偏好或兴趣的评估或预测：	对个人信息主体使用社交网络和其他应用程序的行为进行分析，以便向其发送商业信息或垃圾邮件。
b）使用个人信息进行自动分析给出司法裁定或其他对个人有重大影响的决定：	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，设置针对用户特定偏好的营销计划。
c）系统性的监控分析个人或个人信息，如在公共区域监控、采集个人信息等，但仅在涉及违规事件分析时才使用的视频监测系统除外：	设置在工作场所的 IT 监测系统，监控员工的电子邮件、所使用的应用程序等，用于分析员工工作时间及使用工具（如电子邮件、互联网）的情况
d）收集的个人敏感信息数量、比重较多，收集频率要求高，与个人经历、思想观点、健康、财务状况等密切相关：	通过智能手表、手环、制服、头盔或其它移动设备持续收集或监控个人信息主体的活动、健康相关数据。

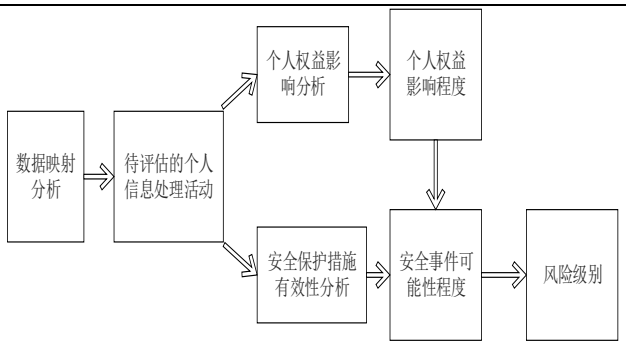
e）数据处理的规模较大，如涉及 100 万人以上、持续时间久、在某个特定群体的占比超过 50%、涵盖的地理区域广泛或较集中等：	社交网络、在线浏览器、有线电视订阅服务大规模收集用户浏览网站、购买记录、观看记录、收听记录等数据。
f）对不同处理活动的数据集进行匹配和合并，并应用于业务：	电商平台、零售商店通过分析顾客的购物、优惠券使用等行为数据，结合顾客的信用数据、第三方和社交网络数据等，获得提高销售额的营销策略。
g）数据处理涉及弱势群体的，如未成年人、病人、老年人、低收入人群等：	能够连接网络的智能玩具收集儿童玩耍的音频、视频数据，或收集儿童的年龄、性别、位置等信息。
h）创新型技术或解决方案的应用，如生物特征识别、物联网、人工智能等：	健身俱乐部、酒店等入口控制系统，指纹支付或刷脸支付等支付程序，通过收集和处理个人信息主体的个人生物识别信息，判断是否拥有进入某些区域、使用某些功能的权限。
i）处理个人信息可能导致个人信息主体无法行使权利、使用服务或得到合同保障等。	提供贷款、信贷、分期付款销售的实体通过收集、处理包含有债务人或类似个人信息主体的数据库信息，针对潜在客户制定信贷决策。

五、个人信息安全影响评估的基本原理及主要流程

(一) 基本原理

开展评估前，需要对评估的对象（可能为某项产品、某类业务、某项具体合作等）进行全面的调研，形成清晰的数据清单及数据映射图表（data flow charts），并梳理出待评估的具体的个人信息处理活动。

开展评估时，通过分析个人信息处理活动对个人信息主体的权益可能造成的影响及其程度，以及分析安全措施是否有效、是否会导致安全事件发生及其可能性，综合两方面结果得出个人信息处理活动的安全风险及风险等级，并提出相应的改进建议，形成评估报告。评估原理示意图如下所示（参见《评估指南》第4.5条）。



评估的规模往往取决于受到影响的个人信息主体范围、数量和受影响的程度。通常，企业在实施该类个人信息安全影响评估时，个人信息的类型、敏感程度、数量，涉及个人信息主体的范围和数量，以及能访问个人信息的人员范围等，都会成为影响评估规模的重要因素。

(二) 主要流程

不管是自评估还是检查评估，两种形式的评估的实施流程是一致的，主要的流程分为九大步骤，详细内容如下表所示。

流程	内容
1、评估必要性分析	包括合规差距评估、尽责性风险评估
2、准备工作	包括组建评估团队、制定评估计划、确定评估对象和范围、制定相关方咨询计划。
3、数据映射分析	在针对个人信息处理过程进行全面的调研后，形成清晰的数据清单及数据映射图表。需要结合个人信息处理的具体场景，开展方式可参考《评估指南》附录 C 中表 C.1《基于处理活动/场景/特性或组件的个人信息映射表》和 C.2《个人信息生命周期安全管理》
4、风险源识别	对要素进行简化，归纳为网络环境和技术措施、个人信息处理流程、参与人员与第三方、业务特点和规模及安全趋势。
5、个人权益影响分析	分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产

	生何种影响，主要包括四个维度：限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、人身财产受损。可参考《评估指南》附录 D.2《评估个人信息主体权益影响程度》。
6、安全风险综合分析	评价安全事件发生的可能性等级，评价对个人权益影响的程度等级，综合考虑安全事件可能性和个人权益影响程度两个要素，综合分析得出个人信息处理活动的安全风险等级。
7、评估报告	编制评估报告。 个人信息安全影响评估报告的内容主要包括：评估所覆盖的业务场景、业务场景所涉及的具体的个人信息处理活动、负责及参与的部门和人员、已识别的风险、已采用及拟采用的安全控制措施清单、剩余风险等。
8、风险处置和持续改进	通常情况下可根据风险的等级，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。
9、制定报告发布策略	包括选取并实施安全控制措施，持续跟踪风险处置落实情况，评估剩余风险等。

六、个人信息安全影响评估报告的用途

实施个人信息安全影响评估，能够有效加强对个人信息主体权益的保护，有利于企业对外展示其保护个人信息安全的努力，提升透明度，增进个人信息主体对其的信任。具体而言，其主要用途包括：

(1) 在开展个人信息处理前，企业可通过影响评估，识别可能导致个人信息主体权益遭受损害的风险，并据此采用适当的个人信息安全控制措施。

(2) 个人信息安全影响评估及其形成的记录文档，可帮助企业在政府、相关机构或商业伙伴的调查、执法、合规性审计中，证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的要求。

(3) 在发生个人信息安全事件时，个人信息安全影响评估及其形成的记录文档，可用于证明企业已经主动评估风险并采取一定的安全保护措施，有助于减轻、甚至免除企业的相关责任和名誉损失。

2020年11月18日，国家信息安全标准化技术委员会召开了《个人信息安全规范》的试点工作启动会，共有15家典型互联网公司被确定为试点单位，从顶层规划、企业管理的各个环节逐步落实个人信息安全规范。《评估指南》作为实施安全规范的重要抓手和切入点，进一步受到相关企业的重视。

实践中，我们已协助一些企业参照《评估指南》实施个人信息安全影响评估的合规自查。对于企业来说，合理评估并处置个人信息处理活动存在的安全风险，是遵循相关法规的合规要求，更是主动应对大数据时代信息风险的应有之义。

杨锦文　合伙人　电话：86-10 8553 7608　邮箱地址：yangjw@junhe.com
高　健　律　师　电话：86-10 8519 1359　邮箱地址：gaojian@junhe.com
李圆圆　律　师　电话：86-10 8540 8665　邮箱地址：liyuanyuan@junhe.com