让子弹飞：网络数据安全风险评估的六问六答

作者：杨迅 | 李依然

个人信息保护合规审计活动如日方升，网络数据安全风险评估又要来了。这是企业不可承受之重，还是可以便捷满足合规要求？

2026 年 6 月 18 日，端午前夜，国家互联网信息办公室、工业和信息化部、公安部三部门联合发布《网络数据安全风险评估办法》(以下简称“**《办法》**”)，将自 2026 年 8 月 20 日起施行。该办法的出台，标志着我国数据安全风险评估制度将很快落地。但是，《办法》对企业到底意味着什么？

一. 《网络数据安全风险评估办法》的性质

从法律位阶来看，《办法》属于部门规章，其上位法依据包括《中华人民共和国数据安全法》《中华人民共和国网络安全法》以及《网络数据安全管理条例》(国务院令第 790 号，以下简称“**《条例》**”)。具体而言，《数据安全法》作为法律，在第三十条确立了“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估”的基本制度；《条例》作为行政法规，第三十一条、第三十三条进一步细化了专项评估和年度评估的具体要求；而《办法》则在前两者基础上，对风险评估的组织实施、程序流程、报告编制、机构管理等操作性事项作出系统规定，构成了“法律—行政法规—部门规章”三层规范体系中最具实操性的下位法规范。

从规范内容来看，《办法》并非创设新的实体性义务，而是对既有法定义务的程序性落实。它明确了风险评估的定义(第二条)、评估主体(第五条)、评估方式(第七条)、报告要求(第十五条、第十六条)、第三方机构管理(第八条至第十四条)以及监督检查机制(第十九条至第二十二条)等。值得注意的是，《办法》第六条明确规定，风险评估工作应当“参照数据安全风险评估有关国家标准开展”，有关主管部门另有规定的从其规定。这意味着 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》(“《评估方法》国标”)等国家标准在评估方法层面具有事实上的规范效力，数据处理者在开展评估时应当予以遵循。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

从《办法》与其他数据保护有关制度的关系看，《办法》是我国数据安全治理体系的重要组成部分，与网络安全等级保护测评、个人信息保护合规审计、个人信息保护影响评估等制度相互衔接，从不同角度规范企业的数据处理活动。

二. 谁要开展网络数据安全风险评估?

《办法》第五条明确了风险评估的义务主体范围，包括强制评估和鼓励评估。

“重要数据处理者”是强制评估的主体。根据《条例》第六十二条，重要数据是指“特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据”。重要数据的处理者由于其处理的数据涉及公共利益或国家利益，依法必须每年度开展风险评估。此外，《条例》第二十八条还规定，处理 1000 万人以上个人信息的数据处理者，也应当遵守《条例》第三十条、第三十二条对重要数据处理者作出的规定，这意味着超大型个人信息处理者同样负有年度风险评估义务。

“一般数据处理者”是鼓励评估的主体。《办法》第五条第三款明确“鼓励处理一般数据的网络数据处理者至少每 3 年开展一次风险评估”。一般数据处理者通常仅涉及私人利益，法律不强制其开展评估，但鼓励其通过定期评估提升数据安全保障能力。这一制度设计体现了比例原则——对涉及公共利益的重要数据处理者课以严格义务，对一般数据处理者则给予更多自主空间。

如何确定重要数据是实践中的一大难题。目前存在三条识别路径：其一，法规直接规定，如《汽车数据安全管理若干规定(试行)》对自动驾驶汽车相关数据的界定；其二，主管部门认定，如国家金融监督管理总局对银行、保险机构重要数据的排摸与认定；其三，企业自我评估，即网络数据处理者按照国家有关规定识别、申报重要数据，由相关地区、部门确认后告知或公开发布(《条例》第二十九条)。对于尚未被明确纳入行业目录的重要数据，企业应当建立内部数据分类分级制度，主动开展重要数据识别工作，避免因识别疏漏而遗漏评估义务。

三. 什么时候应该开展网络数据安全风险评估?

《办法》和《条例》构建了“专项评估”和“定期评估”的触发机制，分别对应“事前节点”和“年度常规”两类时点要求。

专项评估适用于特定数据处理活动发生前。《条例》第三十一条规定，重要数据的处理者在提供、委托处理、共同处理重要数据前，应当进行风险评估，但属于履行法定职责或者法定义务的除外。该条同时列举了六项重点评估内容，包括数据处理目的、方式、范围的合法正当必要性，数据泄露风险，接收方诚信守法情况，合同约束效力，技术和管理措施有效性等。此外，根据《条例》第三十七条，网络数据处理者在境内运营中收集和产生的重要数据确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估——这属于更为严格的国家安全审查程序，与《办法》规定的一般风险评估在性

质和程序上均有区别。《办法》第五条还补充规定,“重要数据安全状态发生重大变化可能对数据安全造成不利影响的，应当及时对发生变化及其影响的部分开展风险评估”，为动态评估提供了依据。

定期评估适用于周期性的对数据处理活动的检视。《条例》第三十三条和《办法》第五条以及第十六条均要求，重要数据处理者应当每年度对其网络数据处理活动开展风险评估，并在评估完成后向省级以上有关主管部门报送风险评估报告。报告内容应当包括数据处理者基本信息、处理数据的目的和方式、安全管理制度及技术措施、发现的风险与事件、数据出境情况等(《条例》第三十三条)。年度评估的周期固定、内容全面，旨在形成常态化的风险监测机制。

值得思考的是，专项评估与定期评估之间如何协调?若重要数据处理者在年度评估后不久即发生提供、委托处理等重要数据流转行为，是否仍需另行开展专项评估?从立法文义来看，专项评估强调的是“事前”时点，与年度评估的“常规”时点各有独立触发条件，原则上应当分别开展。但《条例》第五十二条要求“避免重复评估”，实践中对于短期内连续开展的评估，可在年度评估框架内对新增流转事项进行补充评估，以提高效率、降低成本。

四. 网络数据安全风险评估的目标是什么?

理解数据安全评估的目标，需要将其置于我国数据保护法律体系的整体框架中进行比较分析。《个人信息保护法》确立了“个人信息保护影响评估”(PIA)和“个人信息保护合规审计”两项制度，前者侧重于评估特定个人信息处理活动的合法性、正当性和必要性，识别风险并提出降低措施；后者侧重于对个人信息处理活动全流程的合规性和风险漏洞进行系统性审查。相比之下，网络数据安全评估(针对重要数据及其他非个人数据)似乎综合了上述两者的目标定位，但又具有自身独特的制度内涵。

根据《办法》第二条，风险评估是指“对网络数据和网络数据处理活动安全进行的风险识别、风险分析和风险评价等活动”。这一定义与《评估方法》国标的核心逻辑高度一致，即以数据处理活动为核心，通过识别风险源、分析危害程度与发生可能性、评价风险等级，最终回答“有没有风险、风险是什么、风险在哪里、风险有多大”等根本问题。

从目标层次来看，数据安全风险评估至少包含三个维度：一是合规维度，即审查数据处理活动是否符合法律、行政法规和国家标准的强制性要求；二是风险维度，即识别并评价数据安全事件的发生可能性及其危害后果；三是治理维度，即通过评估发现管理漏洞、优化安全策略、提升整体数据安全治理能力。其最终目标是为本单位决策层和行业主管监管部门做好风险管理提供参考依据。

五. 网络数据安全风险评估谁来做?

《办法》第七条赋予了数据处理者选择权：可以自行开展风险评估，也可以委托第三方评估机构开展。两种模式各有优劣，实践中应当结合数据处理者的能力禀赋、数据敏感程度以及评估复杂度综合判断。

企业自行评估具有显著优势。数据处理者最熟悉自身的业务场景、数据流转路径和系统架构，能够精准识别内部风险点；同时，自行评估避免了向外部机构暴露敏感数据，信息保密最有保障。《办法》第七条要求，自行开展风险评估的“应当指定专人负责”，这意味着企业需要建立内部评估责任制，确保评估工作有明确的责任主体。然而，自行评估也存在局限性：内部人员可能因缺乏独立性而难以客观发现深层问题，技术团队可能缺乏法律合规视角，法务团队又可能缺乏技术检测能力。

委托第三方评估可以弥补上述短板，但是到底谁适合作为合格的第三方也不明朗。尽管 GB/T 45389-2025《数据安全技术 数据安全评估机构能力要求》已于 2025 年 10 月 1 日实施，从基础条件、管理能力、技术能力、人力资源能力、场所与设备资源能力等维度为评估机构设定了能力基准，但《办法》并未明确限定哪类机构具备评估资质，仅“鼓励相关评估机构通过认证”(《办法》第八条)。实际上，数据安全风险评估是一个跨越技术、管理和法律的综合问题——评估中既要审查加密、访问控制、数据脱敏等技术措施，也要判断数据处理“合法、正当、必要”三性，还要评估损害风险和法律环境。单一背景的团队往往难以全面覆盖。

因此，更为现实的路径或许是：以企业自身为牵头主体，组建跨部门评估团队(涵盖业务、安全、法务、合规等职能)，在需要技术检测或法律论证时引入外部专家补充。对于重要数据处理者，尤其是当发生数据安全事件或存在较大安全风险时，主管部门可以要求其委托通过认证的评估机构开展评估(《办法》第十七条)。

六. 如何开展数据安全评估?

《评估方法》国标为数据安全风险评估提供了标准化的方法论框架，可概括为五个阶段：评估准备、信息调研、风险识别、风险分析与评价、评估总结。

评估准备阶段，需确定评估目标(如全面摸排数据资产、识别合规风险或审查特定数据处理活动)、划定评估范围、组建跨部门团队、制定评估方案。信息调研阶段，需核查数据处理者基本情况、业务与信息系统、数据资产(含分类分级情况)、数据处理活动全流程以及现有安全防护措施，形成数据资产清单和数据流图。风险识别阶段，从数据安全管理、数据处理活动安全、数据安全技术、个人信息保护四个维度排查风险源，涵盖制度流程、组织机构、人员管理、数据收集、存储、传输、使用、提供、公开、删除等全生命周期环节。风险分析与评价阶段，对识别出的风险源进行归类，分析危害程度(分为低、中、较高、高、很高五级)和发生可能性(分为低、中、高三级)，最终评定风险等级并形成风险清单。评估总结阶段，编制风险评估报告、提出整改建议、分析残余风险。

实务中笔者常被问及的一个问题是：数据安全风险评估是否与个人信息保护合规审计存在重叠?从制度设计来看，两者的考察对象和目标确有不同——数据安全评估聚焦“重要数据及其他非个人数据”，侧重风险识别与评价；个人信息保护合规审计聚焦“个人信息”，侧重合法合规性审查。然而，对于多数数据处理者而言，重要数据与个人信息往往交织在同一业务系统和数据处理流程中，数据资产的梳理、数据处理活动的排摸、安全措施的审查等工作具有高度共通性。因此，如果能在一次操作中统筹完成两项任务，不失为一种务实高效的选择。

结语

让子弹飞再飞一会儿吧!

如果合规仅仅被视为一项孤立的任务，企业必将不堪重负；如果仅仅依照各类规章和国标，头痛医头、脚痛医脚，企业合规工作同样难以为继。唯一可行的路径，是将数据合规工作嵌入整体工作流程与 SOP，将数据安全考量前置到业务全流程——在数据采集、存储、流转及产品化应用的各个环节，均纳入安全视角。在评估财务风险、权衡收益成本时，将数据安全问题作为必选项；在日常运营中，持续建立数据流转的记录与审查机制。如此，无论是个保审计还是数据安全风险评估，对企业而言都将水到渠成，而非临阵磨枪。

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