数达安全

专 注 数 据 安 全

《网络数据安全风险评估办法》

深度干货解读

2026年6月

01. 发布背景与时间解读

2026年6月18日下午17:00，国家网信办正式发布《网络数据安全风险评估办法》。这一时间点的选择极具深意，延续了监管机构在长假前夕最后一个工作日临近下班时公布重要法规的一贯策略，释放出清晰而审慎的监管信号。

给予市场消化期

旨在为各相关方提供相对集中的时间窗口，用于学习、理解新规条款与核心要求，从而更充分地为后续的合规整改、制度完善等工作筑牢认知基础。

体现监管审慎从容

表明监管机构对法规出台经过了系统调研与深思熟虑，并不追求“突袭式”执法。这种节奏既彰显了法规制定的严肃性，也传递出监管层尊重市场、规范引导的治理思路。

强调合规不容拖延

“节前发布”的安排意味着节后合规工作必须即刻提上日程。监管给予了学习的缓冲期，但绝不代表执行可以放缓，企业需以最快速度启动风险自查与整改落地。

02. 概念演进：“网络数据安全”的法律地位确立

《办法》的出台，标志着“网络数据安全”这一概念在国家级法律法规体系中被正式、反复地确认和强化，为行业监管树立了明确的法律基石。

01 / 首次明确：确立核心概念

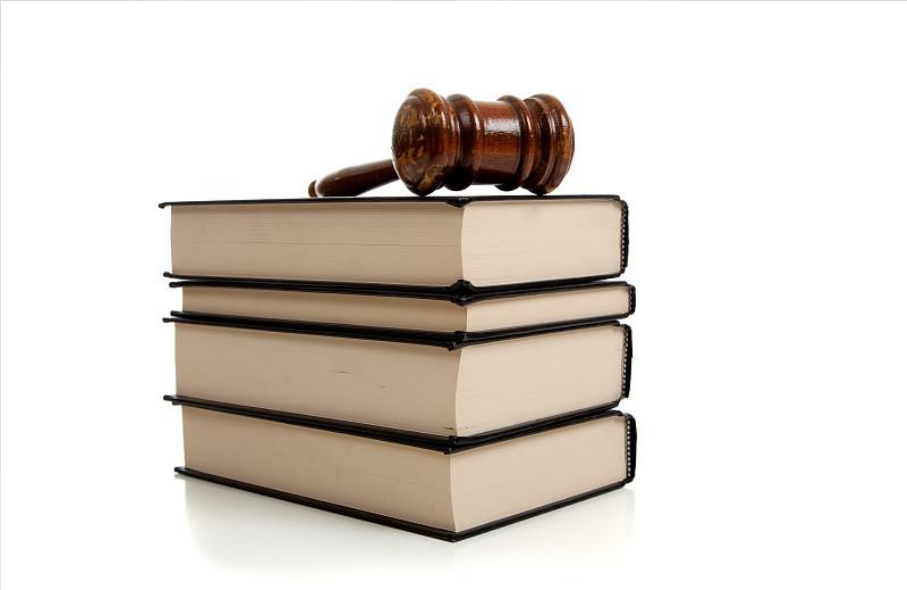
在《网络数据安全管理条例》中，“网络数据安全”首次作为核心概念被提出，重点强调了数据在网络空间流动、处理全流程中的安全特性，奠定了监管的法理基础。

02 / 再次强化：巩固法律地位

本次《办法》直接以“网络数据安全风险评估”命名，从法规名称层面进一步固化概念，彰显了国家对该领域进行专项、系统监管的决心，强化了其独立且核心的法律地位。

监管视角的核心跃迁：从单纯的静态数据“保护”，转向对动态数据“处理活动”的全生命周期风险管控。这一转变深刻反映了国家对网络空间开放性的认知深化，通过体系化的风险评估机制，应对数据安全风险的传导性与放大效应。

03. 适用范围：遵循“长臂管辖”原则



法槌与法典象征着法律管辖的至高权威。无论数据处理**主体身**处何地，只要其业务触及中国境内，就必须接受《办法》的规范与约束。

《办法》**第二条明确**规定：“**在中**华人民共和国境内开展网络数据安**全**风险评估，应当遵守本办法。”这一规定确立了极具延伸性的法律**效力范**围。

主体的广泛性

无论注册地在何处——**中企、外企或海外主体，只要数据**处理活动发**生在境内，均受本**《办法》管辖，**无任何例外**。

行为的关联性

任何在中国境内提供服务、收集数**据的**实体，其相关数据活动均被纳**入**监管范畴，无法置身事外。

💡 对企业的启示：合规即业务边界

企业必须摒弃侥幸心理，将中国的数据合规要求全面纳入全球合规体系，**确保跨境**业务全流程符合中国法律规范。

04. 强制性评估：区分主体类型，明确触发条件

常规强制评估（第五条）

针对**重要数据处理者**，这是一项法定的强制性义务，要求必须每年开展一次数据安全风险评估，确保风险可控、合规经营。

鼓励性评估（第五条）

面向一般数据处理者，采取柔性引导策略，**鼓励至少每3年**开展一次风险评估，**提升数据安全治理能力**，防患于未然。

例外强制评估（第十七条）：触发即强制，委托专业机构

高风险情形：存在较大安全风险，可能危害国家安全、公共利益的，必须启动强制评估。

安全事件触发：发生网络数据安全事件，导致重要数据或大规模个人信息泄露的情形。

监管兜底条款：涵盖法律、行政法规以及有关部门规定的其他应当开展风险评估的情形。

05. 法规定位：并非新增义务，而是明确操作指南

《办法》的出台，并非凭空为企业增设新的法律义务，而是对现有法律要求的具体化、程序化和标准化，旨在将原则性**的上位法**规定转化为可落地、可执行的实践路径。

《数据安全法》第三十条

规定重要数据处理者应当定期开展数据安**全**风险评估，**并按照**规定向有关主管部门报送风险评估报告，**确立了**风险评估的法**定**义务基础。

《网络数据安全管理条例》第三十三条

明确重要数据处理者应当每年度开展一次**数据安全**风险评估，及时处置风险隐患，为风险评估的实施频率和处置要求提供了**具体**规范。

《网络数据安全管理条例》第四十八条

明确行业主管部门对重要数据处理者的风险评估工作负有监督管理职责，构建了“**企**业自评估+监管部门监督”**的双重保障机制**。

结论：《办法》本质上是《数据安全法》和《网络数据安全管理条例》的配套实施文件，它没有创设新义务，而是为企业履行法定的风险评估义务提供了一份清晰、详尽的“**合**规操作手册”。

06. 协同机制：三部门共管，明确网信部门核心枢纽地位

首次确立“网信牵头、多部门协同”的专项工作机制

《办法》第七条开创性地规定跨部门协同共管机制，由国家网信部门会同国务院电信、公安等有关部门建立专项工作机制，统一指导、监督全国范围内的数据安全风险评估工作，从根源上解决多头管理与职责不清的问题。

01. 行业主管部门初审

各行业主管部门负责接收本行业内的数据安全风险评估报告，并进行初步审查，把控行业领域内的合规性基础关。

02. 统一通报同级网信部门

行业主管部门需在规定时限内，将审查后的评估报告通报同级网信部门，确立网信部门作为数据安全管理的最终归口核心。

03. 核心枢纽：共享与协调

网信部门作为核心枢纽汇总全量报告，统筹与电信、公安等部门实现信息共享和工作协调，形成监管合力。

机制价值：有效避免多头重复检查，大幅提升监管效率，同时为企业提供了清晰、唯一的合规报送路径。

07. 行业监管：各司其职，报告报送与监管路径清晰化

《办法》体现“条块结合”监管原则，坚持“谁主管、谁负责”，明确行业主管部门为直接监管主体，构建起从企业报送、主管接收、网信通报至汇总共享的全链路闭环管理体系。

行业主管部门：数据安全监管“第一责任人”

金融、电信、医疗等各行业主管部门，依法对本领域、本辖区内企业的数据安全风险评估工作履行监督、检查与指导职责，确保监管职责落实到具体业务场景，实现专业化、精细化的行业治理。

报告流转机制：公开渠道与法定时效并重

行业主管部门需主动公开报送渠道，保障企业顺利提交评估报告；同时严格遵守“10个工作日内通报同级网信部门”的法定时限，确保信息流转的及时性与合规性，形成监管合力。

01 企业自主报送

企业完成风险评估后，按行业要求向对应主管部门提交合规报告。

02 主管及时接收

主管部门公开报送渠道，及时受理、审核企业提交的评估材料。

03 限时网信通报

自收到报告起10个工作日内，必须向同级网信部门完成通报程序。

04 国家汇总共享

国家网信部门统筹汇总全国评估报告，实现跨部门数据共享与协同。

08. 监督机制：行政检查与社会监督相结合

《办法》构建了一个由行政权力和社会力量共同组成的立体监督网络，通过双轨并行的监督模式，筑牢风险评估的真实性防线。

行政检查核验（第十三条）

主体与权责：省级以上网信、电信、公安、国安等部门，有权对评估报告的真实性、准确性进行检查核验；重要数据处理者必须无条件配合，不得拒绝、阻挠。

社会监督（第十四条）

全民参与监督：任何组织、个人均有权对风险评估活动中的违法违规行为，向履行数据安全监管职责的部门进行投诉、举报，形成全社会共同参与的监督合力。

制度意义：“自上而下”的行政监督与“自下而上”的社会监督形成闭环，构建起全方位、多层次的监督体系，形成强大威慑力，确保风险评估工作不流于形式、不走过场。

09. 法律责任：明确罚则，强化整改与强制措施

法庭场景象征着法律的严肃性与权威性。《办法》以明确**的法律后果**为后盾，确保数据安全评估制度从“纸面规则”**落地**为“刚性约束”。

01. 基础罚则：未评估即违法，严处不怠

未按规定开展风险评估的，将直接依据《数据安全法》《网络数据安全**管理条例》等上位法**处理，面临罚款、责令改正等行政处罚，形成常态**化**监管压力。

02. 强制措施：针对重大风险的“杀手锏”

若重要数据处理活动可能危害国家安全、公共利益，监管部门将首先责**令整改**；对拒不整改或整改不达标的，可依法采取“**停止**处理重要数据”**的**严厉措施。

“停止处理重要数据”实质是业务暂停令。
这是保障业务持续运营的生命线，为所有重要数据处理者敲响了合规警钟，倒逼企业重视并落实安全评估义务。

10. 评估方式：自主评估与委托评估相结合

一般情况（第六条）：灵活选择权

自行评估：适用于具备相应专业能力的企业，鼓励企业建立内生的风险自查体系，降低评估成本。

委托评估：适用于缺乏专业能力或希望获得更客观结论的企业，可聘请第三方机构开展评估工作。

特殊情况（第十七条）：强制委托制

触发条件：当企业存在较大安全风险、发生网络数据安全事件等情形时，评估方式不再有选择权。

核心要求：企业必须委托通过认证的评估机构开展风险评估，以确保评估结果的专业性、权威性和公正性。

制度设计核心逻辑：在日常经营中充分赋予企业自主权，鼓励培养内生自查能力；而在高风险节点上，通过强制引入外部专业力量进行“诊断”，有效弥补企业自查的局限性，构建“自主+监管”双重保障的风险治理闭环。

11. 核心目的：构建“发现-整改-防范”的风险闭环管理

评估不是终点，而是风险治理的起点

《办法》的根本目的并非为了评估而评估，而是通过制度化的评估机制，构建一个从问题识别到整改落实，再到长效防范的动态风险治理闭环，确保数据安全风险可控、可防、可追溯。

01 发现风险：系统识别隐患

通过规范化的评估流程，全面梳理数据处理活动，精准识别数据收集、存储、使用等全生命周期中的安全隐患和合规性风险点。

02 整改问题：限期闭环落实

针对发现的问题，企业需按要求完成整改，并严格在整改完成后的15个工作日内向监管部门报送整改情况报告，确保问题不悬空。

03 防范未来：筑牢长效机制

监管部门通过评估及时发现潜在风险并责令整改，从源头阻断风险向实际安全事件演变的路径，推动企业建立长效的数据安全防范体系。

闭环流程：评估启动 → 风险识别 → 报告编制与报送 → 监管审查与反馈 → 企业整改 → 整改报告 → 持续监控与防范

12. 关键定义：谁是“重要数据处理者”？

《办法》沿用《网络数据安全管理条例》相关规定，采用“目录列明”与“阈值认定”双重标准，清晰界定“重要数据处理者”的主体范围与责任边界。

路径一：处理行业/地方目录列明的重要数据

由各行业主管部门和地方政府发布“重要数据目录”，企业通过自查申报、监管认定的方式，被纳入重要数据处理者管理范畴。

路径二：达到海量个人信息阈值（视同认定）

对于处理个人信息达到1000万人以上的主体，直接视同重要数据处理者，需履行相应的安全保护义务与合规责任。

国民经济运行基石

能源、电网、水利、铁路、民航等关系国家经济命脉的关键行业运营主体。

公共安全与海量用户平台

涵盖三甲医院、疾控中心等公共卫生主体，以及用户超千万的社交、电商、金融支付等大规模互联网平台。

13. 评估机构：明确认证路径，培育专业服务市场

明确认证路径

《办法》第八条明确，鼓励评估机构通过认证确立资质，认证程序严格遵循《中华人民共和国认证认可条例》，为机构资质认定提供了清晰、合规的法律依据和执行标准。

培育专业市场

国家网信、电信、公安等部门将协同发力，积极促进网络数据安全风险评估服务发展，主动培育专业评估机构，推动行业规范化、专业化建设，满足市场合规需求。

指引企业抉择

企业在遴选第三方评估机构时，拥有了明确的判断标尺——即机构是否通过法定认证。这一标准能有效帮助企业筛选出专业能力过硬、服务质量可靠的合规合作伙伴，降低选择风险。

总结：通过明确认证依据与路径，解决了行业资质模糊的核心痛点；同时，国家层面的培育政策将推动专业服务市场的成熟，为数据安全治理体系提供坚实的市场化支撑。

14. 质量保障：多重机制确保评估过程的严肃性

为防止评估工作流于形式、沦为“合规摆设”，《办法》从责任主体、报告规范、过程干预三个维度设立了多重机制，构建起保障评估客观公正的坚实防线。

评估机构的主体责任

依据《办法》第十条，评估机构需公正客观作出风险判断，并对报告的真实性、有效性、完整性承担法定责任，从源头夯实质量基础。

严格的报告形式要求

依据《办法》第十八条，风险评估报告必须由机构主要负责人、评估负责人签字，并加盖机构公章，以规范形式强化报告的严肃性与权威性。

禁止外部不当干预

明确禁止网络数据处理者以任何方式，要求或示意评估机构出具不实、不当的风险评估报告，确保评估过程独立、不受干扰，真正发现潜在问题。

核心价值：通过责任绑定、形式合规与独立性保护的三重约束，确保风险评估结果真实可信，为数据安全治理提供可靠依据。

15. 开放性讨论与思考

尽管《办法》为数据安全评估提供了宏观的法律框架，但在从“纸面上的法”走向“行动中的法”的具体实施层面，仍有诸多关键问题值得行业深入探讨与厘清。

01. 关于监管执法权的具体分工与边界

网信、电信、公安、国安等多部门均承担监管职责，企业亟需明确不同场景下的对接主体与责任优先级，避免出现多头管理或监管空白，确保合规工作有的放矢。

02. 关于评估机构认证的主体与标准

《办法》规定评估机构需通过认证，但认证主体、资质标准及审核流程尚未明确。这是企业选择第三方服务时的核心关切，也直接影响评估结果的权威性与公信力。

这些待解的问题不仅反映了法规落地过程中的现实挑战，更预示着数据安全合规领域将从“框架搭建”走向“精细化运营”，未来的规范体系将更加注重实操性与指导性。

DTS数达安全

专 | 注 | 数 | 据 | 安 | 全

谢谢观看

Q & A

欢迎大家提出问题与建议，共同探讨合规发展路径