重要数据的认定与合规义务

作者：杨迅 | 李依然

《数据安全法》确立了数据分类分级保护制度。重要数据作为承上启下的关键类别，上承核心数据的严格管制，下接一般数据的常规管理，是企业数据合规工作的重心。《网络数据安全管理条例》(国务院令第 790 号，以下简称“《网数条例》”)自 2025 年 1 月 1 日施行以来，重要数据的认定路径、保护义务和出境规则逐步清晰；2026 年 8 月 20 日即将生效的《网络数据安全风险评估办法》(“《风险评估办法》”)进一步明确风险评估义务如何落地。本文围绕三个问题展开：如何认定重要数据、认定后企业承担哪些合规义务、重要数据如何合规出境。

一. 重要数据的认定

(一) 企业自我认定与政府最终确认

《数据安全法》第二十一条规定，国家建立数据分类分级保护制度，由各地区、各部门确定本地区、本部门以及相关行业、领域的重要数据具体目录。也就是说，重要数据的最终认定权在政府主管部门。《网数条例》第二十九条进一步明确，网络数据处理者应当按照国家有关规定识别、申报重要数据，由相关地区、部门确认后告知网络数据处理者，或者向社会公开发布。由此形成重要数据“企业自我认定并申报、政府确认并告知”的基本结构。

这一结构包含两层含义。其一，就日常安全措施而言，企业不能以“未被通知”为由免责。识别、申报重要数据本身是法定义务，企业在获得主管部门确认之前，即应主动开展识别，对疑似重要数据先行采取相应的保护措施；怠于识别、申报而遗漏重要数据的，仍须承担法律责任。其二，就数据出境这一特定场景而言，法规作出了明确的豁免安排：《促进和规范数据跨境流动规定》第二条规定，未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

报数据出境安全评估。换言之，出境评估义务以“被告知”或“公开发布”为触发，企业自我识别出的疑似重要数据，在未获确认前不自动产生出境评估义务。这一安排在强化日常保护与便利数据流动之间取得了平衡，但企业仍应保存识别过程的书面记录，以证明已善尽识别申报义务。

(二) 企业自我认定

企业自我认定重要数据的主要技术依据是国家标准 GB/T 43697-2024《数据安全技术 数据分类分级规则》(“《数据分类分级规则》国标”)。该标准于 2024 年发布实施，为行业主管部门和数据处理者开展数据分类分级提供通用规则，其附录 G《重要数据识别指南》为规范性附录，具有直接的指引效力。

该标准将数据从高到低划分为核心数据、重要数据和一般数据三个级别。重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，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；仅影响组织自身或公民个体的数据，一般不作为重要数据。

在识别规则上，《数据分类分级规则》国标第 6.5 条规定了七项重要数据识别条件，核心逻辑是“影响对象+影响程度”：数据遭破坏后直接对国家安全造成一般危害，或直接对经济运行、社会秩序、公共利益造成严重危害的，即应识别为重要数据；直接关系国家安全、经济运行、社会稳定、公共健康和安全的特定领域、特定群体、特定区域数据，以及达到一定精度、规模、深度或重要性的数据，同样属于重要数据。在此基础上，附录 G 列举了十八项具体识别因素，涵盖未公开的地理与自然资源数据、战略物资储备与产能数据、关键信息基础设施运行及供应链数据、出口管制物项相关技术数据、重要生物资源与群体健康数据、未公开统计数据等，企业可逐项对照排查。

在操作流程上，企业可参照《数据分类分级规则》国标第 7.2 条依次开展：第一步，数据资产梳理，摸清数据资产底数；第二步，制定内部规则——行业主管部门已发布分类分级规则的，优先按行业规则细化执行，没有行业规则或未覆盖的，直接适用国家标准；第三步，实施数据分类与分级，确定核心数据、重要数据、一般数据三个级别的范围；第四步，审核结果，形成数据分类分级清单和重要数据目录并按程序报送；第五步，根据数据重要程度和危害程度的变化动态更新。在认定过程中，企业还应把握三项原则：就高从严，多个因素影响分级时按最高影响程度定级；点面结合，既看单项数据，也评估多源数据汇聚融合后的安全影响；动态更新，数据规模、时效性、应用场景显著变化时重新评估级别。

(三) 部门认定

重要数据由主管部门认定的第一种模式是立法直接确认，以汽车行业为代表。国家网信办等五部门联合发布的《汽车数据安全管理若干规定(试行)》第三条直接列举了六类重要数据：军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量

等数据；车辆流量、物流等反映经济运行情况的数据；汽车充电网的运行数据；包含人脸信息、车牌信息等的车外视频、图像数据；涉及个人信息主体超过 10 万人的个人信息；以及有关部门确定的其他数据。该规定同时明确重要数据应当依法在境内存储。“立法列举”模式下，企业可直接对照条文“对号入座”，认定标准最为清晰。

重要数据由主管部门认定的第二种模式是“调研排摸—机构申报—确认通知”，以金融行业为典型。国家金融监督管理总局发布《银行保险机构数据安全管理办法》，要求银行保险机构建立数据分类分级保护制度，制定并及时更新重要数据目录，向监管部门报送。实践中，监管部门先通过调研排摸掌握行业数据底数和识别口径，机构据此自我认定并申报目录，监管部门再审核确认，将认定结果告知机构，形成本机构的重要数据清单。这种模式下，企业认定是起点、监管确认是终点，二者持续互动。

此外，工业和电信领域依据《工业和信息化领域数据安全管理办法(试行)》实行重要数据和核心数据目录备案管理；自然资源领域对测绘地理信息数据另有专门管制。重要数据认定的总体趋势是，各地区、各部门正陆续发布本行业、本领域的重要数据目录，企业应密切跟踪目录动态，及时校准自身认定结果。

二. 重要数据的合规义务

重要数据一经认定，数据处理者即须在《数据安全法》和《网数条例》框架下承担一系列强化义务，可归纳为六个方面。

(一) 组织架构

《数据安全法》第二十七条第二款要求，重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。《网数条例》第三十条进一步细化了任职要求：数据安全负责人应当由管理层成员担任，具备数据安全专业知识和相关管理工作经历，并有权直接向网信部门、公安机关等主管部门反映数据安全情况；数据安全管理机构负责制定实施管理制度和操作规程、组织教育培训、监测和处置安全风险、受理投诉举报等工作。依据《网数条例》第二十八条，处理 1000 万人以上个人信息的数据处理者，即使不处理重要数据，也应遵守前述规定。企业落地时，应保证数据安全负责人实质性参与经营决策、拥有与责任相匹配的资源调配权，避免“挂名化”。

(二) 制度建设

《数据安全法》第二十七条确立了“建立健全全流程数据安全管理制度、组织开展数据安全教育培训”的基本要求；《网数条例》第九条进一步明确，应在网络安全等级保护的基础上建立健全网络数据安全管理制度。对重要数据处理者而言，其制度体系至少应包括：其一，数据分类分级制度，明确重要数据的识别、申报、目录管理和动态更新流程；其二，全流程管理制度，覆盖数

据收集、存储、使用、加工、传输、提供、公开、删除各环节的操作规程和审批要求；其三，对外提供与委托处理管理制度，将提供、委托处理、共同处理重要数据纳入事前专项评估和合同约束；其四，应急处置制度，建立事件分级、响应、报告和演练机制；其五，人员管理制度，以教育培训和保密义务约束接触重要数据的员工。此外，《网数条例》第三十二条规定了特殊情形的报告义务：重要数据处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障数据安全，并向省级以上有关主管部门报告重要数据处置方案和接收方信息。

(三) 技术措施

《数据安全法》第二十七条要求数据处理者采取相应的技术措施和其他必要措施；《网数条例》第九条列举了加密、备份、访问控制、安全认证等代表性措施。总体而言，技术措施应与数据重要程度相匹配：存储环节实施加密存储和备份；使用和传输环节通过访问控制、身份认证、传输加密防止未授权访问；共享和提供环节辅以脱敏、水印、接口鉴权等手段。日志留存与安全审计是各项措施有效性的基础，应确保对重要数据的操作全程留痕、可追溯。还应注意，《风险评估办法》第二十三条要求，涉及重要数据加密等技术措施的，应按国家密码法律、行政法规要求开展商用密码应用安全性评估。

(四) 风险监测和处置

《数据安全法》第二十九条规定了双层义务：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。重要数据处理者应将风险监测常态化，通过漏洞扫描、入侵检测、异常行为分析等手段持续掌握重要数据安全状态；建立应急响应机制，明确事件分级标准和报告时限，确保“处置、告知、报告”同步到位；事后开展溯源分析和整改复盘，并将事件及处置情况纳入年度风险评估报告，形成“监测—处置—复盘—改进”的闭环。

(五) 风险评估

《数据安全法》第三十条规定，重要数据的处理者应当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报告，报告应包括处理的重要数据的种类、数量、开展数据处理活动的情况、面临的风险及其应对措施等。《网数条例》和 2026 年 8 月 20 日起即将施行的《风险评估办法》将该义务具体化为“年度评估+专项评估”的双层结构。

日常评估即年度评估。《网数条例》第三十三条要求重要数据处理者每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送报告。《风险评估办法》进一步明确：评估可自行开展(须指定专人负责)，也可委托第三方评估机构；评估参照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》等国家标准实施；年度评估完成后 20 个工作日内报送报告，报告至少保存 3 年。

专项评估对应特殊情形：一是《网数条例》第三十一条规定，提供、委托处理、共同处理重要数据之前，应当进行风险评估，重点评估处理目的的合法正当必要性、数据安全风险、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(履行法定职责或法定义务的除外)；二是《风险评估办法》第五条规定，重要数据安全状态发生重大变化可能造成不利影响的，应当及时对变化部分开展评估。专项评估与年度评估各有独立触发条件，原则上分别开展，实践中可在年度评估框架内对新增事项作补充评估，避免重复投入。

(六) 数据出境安全评估

重要数据出境不适用一般风险评估，而须通过专门的国家安全审查程序。《数据安全法》第三十一条确立了重要数据出境监管的制度框架，《网数条例》第三十七条明确，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。按照《促进和规范数据跨境流动规定》第七条，关键信息基础设施运营者向境外提供个人信息或者重要数据，以及其他数据处理者向境外提供重要数据，均须申报出境安全评估，且不设数量门槛——只要涉及重要数据即须申报。安全评估由国家网信部门组织实施，具有事前准入性质，未通过评估的重要数据不得出境；评估结果有效期为 3 年，符合条件的可以申请延长。

三. 重要数据出境合规

重要数据出境合规可分为“出境前的基础安排”与“出境通道的合规运用”两个层面，前者解决数据和访问在哪里，后者解决数据如何依法跨境流动。

(一) 出境合规的基础

1. 本地化部署

重要数据的制度基调是“原则上境内存储，出境为例外”。本地化存储是对重要数据开展监管的基石，如果企业采用无服务器模式(Thin Terminal Mode)，重要数据一旦产生就出境，监管也无从着手。《汽车数据安全管理若干规定(试行)》第十一条亦规定重要数据应当依法在境内存储，确需向境外提供的应当通过安全评估。“确需”二字表明，重要数据的本地化是默认状态，出境须以业务必要性为前提接受个案审查。

对跨国企业而言，本地化部署是出境合规的物理基础。很多外企已陆续在境内设立数据中心，将中国业务数据存储于境内，仅将经评估准予出境的数据项传输至境外。本地化部署也直接影响出境评估的可行性：《数据出境风险自评估报告》要求说明拟出境数据在境内存储的系统平台、数据中心及出境链路，如果境内缺乏清晰的存储和链路架构，数据出境安全评估的申报将无从谈起。企业规划 IT 架构时，应尽早实现境内外数据分域存储、分级部署，避免“架构先行、合规补课”。

2. 本地访问权限控制

重要数据的本地化存储同时需要本地的权限控制。如果本地化存储的重要数据的最高管理权限在境外，实际上意味着境内主体无法控制境外获取和处理数据的行为，我国监管部门也就难以管辖重要数据的处理。

《数据出境安全评估申报指南(第三版)》明确，数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出的，即属于数据出境行为。境外母公司、全球研发团队、境外 IT 运维人员对境内系统的远程访问，本身就是一条“逻辑出境”通道，不因数据物理上存放于境内而豁免。

可见，访问权限控制是出境合规的第二块基石。企业应建立面向境外访问的专门管控：其一，最终管理权限必须在境内，实现对境内重要数据的控制；其二，通过最小必要授权，境外人员才能访问境内重要数据；其三，访问行为全程留痕，通过日志审计、堡垒机录屏等形成可核查的访问台账；其四，采取技术隔离措施，对确需向境外开放查询的场景，优先采用脱敏查询、接口受控调用等方式替代直接的数据库访问。权限控制到位，既是防止“未申报即出境”的防火墙，也是出境必要性论证的事实基础。

(二) 出境路径

1. 安全评估的简要流程

重要数据出境的法定通道是申报数据出境安全评估。依据《数据出境安全评估申报指南(第三版)》：数据处理者首先开展出境风险自评估并形成自评估报告；随后通过数据出境申报系统(sjcj.cac.gov.cn)线上提交申报材料(关键信息基础设施运营者等特殊主体线下经省级网信办申报)；省级网信办 5 个工作日内完成完备性查验，通过后提请国家网信办受理，国家网信办 7 个工作日内确定是否受理；受理后组织评估，期间可要求补充或者更正材料；评估完成后出具评估结果通知书，有异议的可在 15 个工作日内申请复评。评估结果有效期为 3 年，届满前 60 个工作日内，在出境目的范围、出境主体均未变化且数据规模增幅不超过 20%等条件下，可以申请延长。

2. 不能“全员出境”

安全评估按业务场景逐项审查数据项，结论是“逐项放行”而非“整体通过”。企业不能一揽子将重要数据全部出境，必须分场景开展必要性评估，只有必须出境的才能出境。国家网信办公布的数据印证了这一点：截至 2025 年 3 月，涉及重要数据出境的 44 个评估项目中，申报的 509 个重要数据项经评估准予出境的为 325 项，仅占申报数据项总数的 63.9%，另有 7 个项目整体未获通过。企业应树立“能不出境的不出境、能少出境的不多出境”的预期，申报前即对拟出境数据项进行内部筛选和压缩。

3. 必要性评估

必要性是评估审查的核心。自评估报告须以列表形式逐项列明数据项名称、内容描述和出境必要性，逐一说明该数据项为何必须出境、境外接收方为何必须使用；数据出境的目的、范围、方式须具备合法性、正当性、必要性，并与境外接收方处理数据的用途、方式相匹配。必要性论证空泛、数据项与业务场景缺乏对应关系，是安全评估无法获得国家网信办通过或被要求压缩出境范围的常见原因。

4. 内控制度

通过安全评估不等于一劳永逸。企业还须：一是建立出境数据台账，严格按照评估结果通知书确定的目的、范围、方式和数据种类规模开展出境活动，留存记录备查；二是动态管理，出境目的、范围、接收方等发生变化的应当重新申报，有效期届满需继续出境的及时申请延长。

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