数据要素合规流通的风险评估与防范

王小乾

（天翼云科技有限公司，北京 100083）

摘要：聚焦于数据作为关键生产要素在数字经济时代所面临的合规流通挑战，对数据要素合规流通中的风险评估与防控对策进行了研究。尽管我国政府已出台《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法规引导数据合规使用，但仍存在隐私保护、数据安全、法规滞后、跨境数据流动管控以及新技术风险等方面的难题。因此，提出一套严谨的风险评估方案，并就合规风险给出了相应策略。

关键词：合规流通；合规风险评估；隐私保护；合规管理体系

中图分类号：F27；G259；D922. 16　　**文献标志码**：A

引用格式：王小乾. 数据要素合规流通的风险评估与防范[J]. 信息通信技术与政策，2024，50(4)：41-46.

DOI：10. 12267/j. issn. 2096-5931. 2024. 04. 006

0　引言

随着数字经济的迅速崛起，数据要素在社会经济体系中的核心地位日益显著。数据作为一种与资本、劳动力和技术并驾齐驱的关键生产要素，已经成为驱动全球经济和社会进步不可或缺的动力源泉。尽管我国已确认数据为关键生产要素，但是出于对安全和隐私合规的考虑，各主体所持数据呈现出分散存储、碎片化处理的特点[1]，数据要素的合法、合理、安全流通不仅关系到个人隐私权的有效保护和信息安全的维护，更对国家安全战略、经济发展态势以及社会稳定性有着深远影响。

本文深度探索数据要素合规流通中的各类风险，并构建科学的风险评估框架，制定可行的防控策略，旨在为政策/法规的制定和实践操作提供理论指导与洞见分析，推动数据治理体系的持续完善与创新发展。

1　数据要素合规流通的背景与现状

1.1　数据要素市场的形成与发展

在数字化进程中，互联网、物联网和人工智能等技术的广泛应用深刻改变了数据产生、收集和利用的方式。社交媒体、电子商务等领域数据量急剧增长，形成了具有显著商业价值和社会价值的数据资源库。以我国为例，据互联网数据中心（Internet Data Center，IDC）数据显示，预计到 2027 年，我国数据量将以年均 26. 3%的速度增至 76. 6 ZB，居全球首位[2]。

在数字经济时代，数据要素市场扮演着核心角色，其发展不仅能驱动经济增长，更深度影响着社会治理与个体生活质量。这一市场的形成与发展获得了政府、企业和社会的广泛关注和支持，政策层面，各国政府积极出台措施鼓励市场健康发展，旨在创建利于数据开放共享流通的环境，并通过强化数据安全和隐私保护监管，确保合规性和可持续性；企业方面，则加大投资整合开发数据资源，运用数据驱动决策创新，提升竞争力，拓展新业务领域。

1.2　国内外政策环境对数据要素合规流通的影响

国内外政策环境分别从“严格细致”和“灵活开放”两个维度对数据要素市场的合规流通提出了具体要求，企业在国内外运营时需适应不同的政策环境，采取相应策略措施确保数据流通合法合规。

国内层面,我国政府通过出台《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等系列法律法规,明确规定了数据的权利义务、处理行为规范,有效保障了个人隐私和企业秘密安全。同时,国家发布《促进大数据发展行动纲要》《数据安全管理办法(征求意见稿)》等政策文件,积极鼓励数据开放共享及流通交易,《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》提出建立合规使用的数据产权制度,以及合规高效、场内外结合的数据要素流通和交易制度[3],为数据要素市场的健康发展提供了清晰的政策指导和广阔的市场空间。

国外层面,欧盟以《欧盟数据保护通用条例》(General Data Protection Regulation,GDPR)为代表的数据保护法规体系严格规定了数据收集、存储和使用行为,并强调数据主权和隐私权益保护,严格限制跨境数据流动。美国则采取更为灵活的政策策略,重视市场机制和行业自律,虽同样出台了相关法律来规范数据处理行为,但相对更注重国家安全和隐私权益的动态保护管理。

1.3 数据要素合规流通所面临的多元化挑战

数据要素合规流通面临着涉及隐私保护、数据安全、法律法规适应性、跨境数据流动监管和技术发展带来的合规风险以及企业合规意识与能力提升等多层面挑战。在隐私保护与数据安全层面,大数据时代如何平衡个人隐私保护与合理利用成为突出难题,频繁的泄露事件更凸显了其紧迫性;法律法规层面,现有法规往往滞后于技术迭代和市场变化,法规的修订和完善以及有效执行成为巨大挑战。

在全球化背景下,跨境数据流动监管因各国政策差异而复杂艰巨,需国际间加强合作,共同制定统一标准以促进数据要素的合规流通。随着新技术如人工智能、区块链的应用,数据流通方式发生变化,如何借助新技术提高数据流通效率和安全性,并避免出现新的合规风险,需要多方协作来推动技术创新和应用。

此外,尽管政府和社会对数据合规日益重视,部分企业仍存在合规意识和能力不足的问题。因此,有必要通过政府引导、行业协会推动和社会教育等方式,强化企业合规文化建设,提升企业遵守法律法规的自觉性,以实现数据要素的合规流通。

2 数据要素合规流通的合规风险评估

2.1 数据的敏感性风险评估

数据要素的合规流通中,数据敏感性风险评估扮演着核心角色,直接关联到数据保密性、完整性和可用性保障。数据敏感性风险评估通过分类分级识别数据机密程度,针对不同敏感度的数据(如个人隐私、商业秘密、国家安全信息)设定相应的保护要求和合规基准,为风险管理提供基础。数据敏感性风险评估应紧密结合具体业务场景和行业合规标准,实施定制化的风险评估,并定期复查更新,以适应业务发展和法规要求的变化。综合考虑数据敏感性级别、生命周期管理及内外部风险因素,科学地开展数据敏感性风险评估有助于企业或机构构建完善的数据安全管理体系,有效保障数据要素的合规流通与使用。

2.2 数据的隐私保护风险评估

在数据隐私保护风险评估过程中,需要确保个人隐私权益不受侵害。主要包含如下几点。

(1)隐私设计评估。审视企业在产品或服务设计初期是否遵循隐私保护的设计原则,如最小化原则、透明度原则、用户控制原则等。

(2)隐私政策与协议审查。详细审核企业发布的隐私政策及与用户签订的服务协议,确认其中是否清晰列明了个人信息收集、存储、使用、共享、转让、公开披露等各环节的具体操作流程,以及针对用户隐私权利的相关保障措施。

(3)匿名化与去标识化技术评估。考察企业是否采用先进的匿名化和去标识化技术对敏感信息进行处理,以降低直接识别特定个人的可能性,并评估这些技术的实际应用效果。

(4)隐私泄露应急响应机制评估。检查企业是否建立了完善的隐私泄露事件应急预案,能否迅速、有效地发现并处置潜在的数据泄露问题,同时评估企业对于发生泄露后的通知义务履行情况及其对受影响用户的补偿措施。

(5)员工教育与培训效果评估。基于 2023 年 Verizon 数据泄露调查报告(Data Breach Investigations Report,DBIR)的关键发现,74%的安全事件中存在显著的人为因素[4],组织内部行为以及员工对于安全策略的理解和执行成为了诱发数据泄露的主要源头之

一。因此，需要评估企业是否定期开展针对员工的隐私保护知识培训和意识提升活动，评估此类活动对企业内部良好隐私保护文化形成的作用及实际成效。

2.3 数据的合规性审查

对数据要素的合规性风险进行全面而深入的审查是确保企业在数据生命周期的所有环节，即从数据的收集、存储、处理、共享、传输直至使用阶段，均严格遵守相关法律法规及行业规范的重要保障。

（1）数据收集的合规性审查。对数据采集的目的、手段、范围进行合法性验证，确保获取用户充分知情同意，遵循最小必要原则等法律规定。

（2）数据存储的合规性审查。评价企业在数据储存环节的安全措施是否达到法定标准，如加密技术的运用、访问权限控制策略以及备份恢复机制的有效性，以确保数据存储过程中的安全性、完整性和可追溯性。

（3）数据处理的合规性审查。深入检查数据处理活动，如清洗、分析、挖掘等多种操作是否合法且适度，防止发生超越授权或非法处理的现象，同时关注并提升数据质量和准确性。

（4）数据共享与传输的合规性审查。严谨核实跨国数据流动的合法合规性，符合 GDPR、《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）等国际和国内法规，并对合作方的数据安全管理能力实施详尽评估，通过签署含保密条款在内的合规合同来保障数据流转的安全。

（5）数据使用的合规性审查。保证数据的实际用途与最初收集目的保持一致，避免未经许可的用途，尊重和维护个人数据主体的合法权益。

（6）内控制度建设与流程优化。设计并完善企业的内部数据合规管理制度，涵盖但不限于数据分类分级制度、权限管理制度、独立审计监督机制等，使合规要求在具体业务操作层面得到贯彻执行。

（7）动态监测与持续改进机制。定期组织内部自我评估和第三方独立审计，及时发现并有效应对潜在合规风险，紧跟法律法规更新的步伐，持续调整和优化企业的合规管理体系。

2.4 数据的交易与共享风险评估

风控指数作为一种综合性评估工具[5]，特别针对区域内的数据要素交易平台、数据本身、云计算网络以及资金流动的安全防控和安全能力状态提供了量化的评价体系。这一指数设计包含了 4 个核心评估维度，每个维度都反映了数据交易与共享活动中不同的风险因素和防控要点。

平台安全维度着重评估数据交易平台的安全性和稳定性。这一维度的评估内容主要包括平台是否配备了高效的熔断机制以应对突发流量或异常交易行为，平台是否通过了权威的安全认证，其系统架构的鲁棒性以及平台整体的安全运维水平和抗风险能力如何。

数据安全维度专注于数据本身的健康状态与合规性。该维度评估数据在共享、开放和交易活动中的安全性，考察数据的质量、完整性和一致性，同时深入审视数据的采集、处理、存储和使用是否遵循了相关法律法规以及行业标准，确保数据交易的合法性与合规性。

云网安全维度聚焦于云计算基础设施和网络通信环境的安全状况。这部分评估内容主要围绕数据存储的安全防护措施和数据在网络传输过程中的安全保障机制，旨在确认数据在云端和网络环境中的传输与存储风险得到了有效控制。

资金安全维度则关注与数据交易相关的资金流动安全性，确保交易资金的来源合法、支付渠道安全可靠，防止在交易结算过程中发生欺诈、洗钱等非法行为。

3 合规风险的防范与应对策略

3.1 建立健全合规管理体系

合规风险的防范与应对策略在数据要素合规流通稳健发展的过程中起着决定性作用。其中，建立一套全面而严谨的合规管理体系尤为关键。这一管理体系旨在为组织提供系统化和规范化的手段，以识别、评估并有效管理各类合规风险，以下是关于如何建立合规管理体系的一些建议。

一是构建合规能力体系与目标。此能力建设应包括数据合规风险识别、数据分类分级、个人信息主体权利保障、网络安全和数据安全、合作方管理以及员工个人信息保护等方面[6]。体系的目标在于保障企业的各项业务活动、产品及服务严格遵循法律法规、行业标准以及道德规范的要求。

二是制定合规政策与流程。这些政策和流程需明确规定企业在处理数据过程中的各个环节，包括但不限于数据收集、存储、处理、共享及使用时，所应遵守的合规性准则。同时，还应包含针对不合规行为的发现、报告

及处置机制,以确保任何潜在问题能够得到及时解决。

三是设立合规管理团队。该团队需具备必要的专业知识与实践经验,能够独立、客观地进行合规风险的评估与管理。为保证团队的有效运作,企业应提供充分的资源支持,涵盖培训、预算投入和技术工具等方面。

四是重视外部沟通合作。通过持续和监管机构、行业协会、客户及合作伙伴等的信息交流与合作,企业可获取最新的合规要求和最佳实践,从而更好地适应不断变化的合规环境。

五是定期审查与更新。企业根据内外部环境的变化、法律法规的修订及最佳实践的发展,对现有的合规政策、程序及措施进行系统性评估与调整优化。通过定期审查,识别潜在的合规风险缺口和管理失效,确保体系始终契合最新的法律要求和技术标准;而适时的更新,则旨在改进和完善合规管理制度,强化风险防控能力,从而维持组织在数据要素流通领域的持续合规状态。

六是合规意识与文化培养。借助于培训、宣传及教育活动,使员工深入理解合规的重要性,并熟练掌握如何在日常工作中遵循相关规定。唯有当全员都能自觉遵守合规要求时,合规管理体系才能真正发挥其效用,支撑企业的健康发展。

3.2 加强数据安全与隐私保护措施

强化数据安全和隐私保护措施在数据要素合规流通的风险应对策略中占据核心地位。鉴于近年来数据泄露及隐私侵犯事件的频繁发生,企业对数据安全保障及隐私保护的关注度显著提升。以下将详细阐述加强数据安全与隐私保护的具体措施。

首先,构建健全的数据安全与隐私保护制度是基础环节。此制度需明确规定数据生命周期各阶段的安全标准和隐私保护要求,明确不同岗位的角色权限,确保敏感信息仅能由授权人员访问。

其次,运用先进的加密技术和安全防护机制以增强技术层面的安全屏障。企业应采用有效数据加密方法确保静态存储和动态传输过程中的数据机密性和完整性,并结合数据沙箱、隐私计算、使用控制、区块链等技术实现数据产品安全开发保障[7]。同时,部署防火墙、入侵检测系统等防御设施,阻止未经授权的访问行为和抵御潜在恶意攻击。定期开展系统的安全性评估和审计,验证并持续优化安全措施的有效性。

再次,注重员工培训教育以提高内部的数据安全意识与操作水平。鉴于员工行为是信息安全防线中的关键环节,组织应定期举办培训课程、模拟演练以及宣传活动,使员工深刻理解数据安全与隐私保护的重要性,掌握必备的安全操作规程和应对策略。

另外,企业在数据流通过程中应与客户和合作伙伴签订详尽的数据安全与隐私保护协议。在数据共享、交换或交易情景下,明确各方在数据使用、保密义务和违约责任等方面的权利与约束,通过契约机制构建互信环境,确保所有参与者能够遵循法律法规,进行合法、合规的数据处理活动。

最后,面对不断演变的技术环境和日趋严格的法规要求,企业应保持敏锐的洞察力和适应性,及时跟进最新的安全威胁情报和合规发展趋势,适时调整并完善自身的数据安全与隐私保护策略。同时,积极参与行业交流与合作,共同推动数据安全与隐私保护理论与实践的发展。

3.3 提升合规意识与培训力度

提升合规意识与培训力度是防范与应对合规风险的重要手段。通过加强员工对合规要求的认知和理解,可以降低因违规行为带来的风险和损失。提升合规意识与培训力度的相关措施包括以下几点。

一是加强高层管理人员的合规意识培养。高层管理人员是企业的决策者和引领者,其合规意识的高低直接影响到整个企业的合规文化。因此,应加强对高层管理人员的合规培训,提高其合规意识和责任感。通过制定明确的合规政策,鼓励高层管理人员积极推动合规文化的建设和发展。

二是建立完善的合规培训体系。该体系应覆盖不同层级和部门的员工,确保每个人都有机会接受合规培训。培训内容应包括法律法规、行业标准、公司规章制度等方面的知识,以及实际操作中的合规要求和案例分析。同时,应定期开展合规培训,确保员工能够及时了解最新的合规要求和风险点。

三是注重培训效果评估和反馈。仅仅开展培训是不够的,还需要对培训效果进行评估和反馈。通过考试、问卷调查等方式,了解员工对合规知识的掌握程度,以及在实际工作中的运用情况。根据评估结果,及时调整和完善培训内容和方法,确保培训的有效性和针对性。

四是建立合规奖励与惩罚机制。为了激励员工自觉遵守合规要求,企业应建立相应的奖励机制。对于在工作中表现突出的员工给予表彰和奖励,树立榜样

作用。同时，对于违规行为应进行严肃处理，包括警告、罚款、解除职务等措施，以维护企业的合规形象和信誉。

五是积极营造合规文化氛围。通过开展各种宣传活动、举办合规知识竞赛、制作宣传资料等方式，让员工在日常工作中时刻感受到合规的重要性。同时，领导层应以身作则，积极践行合规要求，为员工树立良好的榜样。通过营造浓厚的合规文化氛围，使员工自觉遵守合规要求，降低违规行为的发生概率。

3.4 建立风险预警与快速响应机制

建立风险预警与快速响应机制在防范与应对合规风险中扮演着核心角色，也是企业有效应对潜在合规风险、降低损害的关键环节。以下从 4 个方面详细阐述构建这一机制的具体措施。

首先，构建完善的风险预警系统。系统应当具备实时监测和智能分析的功能，通过对企业内部和外部环境产生的大量数据进行深入挖掘，及时识别可能存在于数据收集、存储、处理、共享及使用等全生命周期中的合规风险隐患。通过预先设定风险阈值和评估指标，系统能够在风险即将触发时自动触发预警信号，利于企业迅速察觉并着手应对潜在风险。

其次，建立快速响应机制。应明确风险响应流程及责任分工，设立清晰的决策层级与沟通渠道，确保各级别、各部门职责分明，能够在第一时间启动响应行动。制定详细的应急预案，预案中包括但不限于识别风险等级、评估影响范围、确定应对策略以及具体操作步骤，以便于在风险事件发生时快速决策与执行。通过定期进行模拟演练和培训，强化员工对响应流程的理解和熟悉度，提升团队协作与应急反应能力。根据实际运行效果和外部环境变化，持续优化和完善响应机制，引入先进的管理理念和技术手段，以提高快速响应的精准性和有效性，最终实现对合规风险的高效防控。

再者，强化与外部利益相关者的沟通与合作。其中包括但不限于监管机构、行业协会、客户和合作伙伴等多元主体。及时向外界通报风险情况，不仅可以争取更多来自外部的支持与资源，还有助于形成共同应对风险的合作态势。同时，通过与其他组织间的交流互动，分享风险信息、成功经验和最佳实践，有助于提升整个行业的合规管理水平。

最后，持续改进与优化。风险预警与快速响应机制并非一劳永逸，而是需要根据外部环境的变迁和技术进步持续更新，定期评估既有机制的有效性，结合实际情况进行适时调整和创新，通过引入先进的信息技术手段和科学的管理方法，不断提升风险预警的精准度和快速响应的效能，确保企业始终保持在合规风险管理的最前沿。

4 案例分析

在数据要素合规流通这一重要领域，国内外涌现了众多具有深刻启示意义的案例。这些案例不仅提供了宝贵的实践经验，也为其他组织的数据合规实践提供了参考依据。本文将选取有代表性的典型案例进行深入剖析，以进一步强调数据要素合规流通的重要性及其实施策略。

国内层面，聚焦于我国成功践行数据要素合规流通的企业之一——淘宝网（阿里巴巴集团旗下的电商平台）。据《中国网络法治发展报告（2019）》，淘宝网在数据合规管理方面表现出色，其用户数据保护措施具有很高的示范性。淘宝网严格遵循相关法律法规，对数据的收集、存储、处理和使用进行了明确的规定和限制，并确保所有操作流程均符合国家与行业的合规要求。此外，平台还与第三方合作方签订了严格的保密协议，通过法律手段约束合作方对用户数据的获取和使用，从而保障数据在流转过程中的安全性。更为关键的是，淘宝网充分尊重并保障用户的知情权和处置权，允许用户自主选择导出或删除个人数据，这一举措大大降低了用户数据泄露的风险，有力提升了用户对平台的信任度和满意度。

国外层面，本文从正面和反面两个维度进行分析。正面案例参照欧洲跨国企业 SAP 公司的成功经验。根据《哈佛商业评论》（2020 年 7 月刊）报道，SAP 在 GDPR 出台后，迅速对其全球业务进行了调整优化，制定了一套严谨的数据安全管理体系。该公司不仅强化了内部数据分类与权限管理，还在产品设计阶段就融入了隐私保护理念，同时加强了与合作伙伴的数据共享监管，确保在全球范围内实现了数据要素的合规流通。

在反面案例中，Facebook 用户数据泄露事件无疑是最具警示性的案例之一。2018 年，《纽约时报》等多家国际主流媒体曝光，Facebook 因软件漏洞导致约 8 700 万名用户的个人信息被黑客窃取，引发了全球范围内的广泛关注与严厉谴责。此次事件暴露出企业在数据要素

合规流通方面的严重疏漏,包括未及时发现和修复系统漏洞、对第三方应用程序接口监管不力以及在发生泄露后应急响应迟缓等问题。这一案例对企业提出了警告,表明企业必须更加重视并投入资源来加强用户数据的安全保护,完善技术防范措施,严格执行与第三方的合作条款,才能有效防止大规模数据泄露事件的发生。

5 结束语

本文深度探究了数据要素合规流通所面临的复杂挑战与风险,全面梳理了企业在数据要素合规流通过程中可能遭遇的多元化风险因素,提出了一整套精细化的风险防控与改进策略。为全面评估数据要素的合规风险,企业需要建立健全合规管理体系,并通过先进技术手段来强化安全保护措施,以保障数据的机密性和完整性;同时,需明确与合作伙伴之间的数据合规要求与操作规范,共建数据安全防护联盟,以实现风险共担与协同防御;此外,应将数据合规培训嵌入企业常规教育体系之中,全面提升全员对数据合规性的认知与实践能力,确保合规文化深入企业内部。最后,本文还提出了建立风险预警和快速响应机制的重要性,以降低合规风险的发生概率。而针对合规的持续改进与优化措施,需要进一步研究和分析,并结合企业的实际业务情况,给出更加精确和贴合实际的方案。

参考文献

[1] 中国信息通信研究院, 中国广告协会, 蚂蚁科技集团股份有限公司. 数字广告数据要素流通保障技术研究报告(2023 年)[R], 2023.

[2] 互联网数据中心. IDC 正式发布数据云报告,中国数据量规模年增速全球第一[EB/OL]. (2023-05-28)[2024-01-10]. https://www.eet-china.com/newsexpress/70706.html.

[3] 中国信息通信研究院. 数据要素白皮书(2023 年)[R], 2023.

[4] DBIR. 2023 data breach investigations report[R], 2023.

[5] 王丹阳, 侯宁. 数据要素市场建设中的企业数据合规分析[J]. 信息通信技术与政策, 2023,49(4):42-47.

[6] 中国信息通信研究院, 贵州大学公共大数据国家重点实验室, 贵州财经大学. 数据要素交易指数研究报告(2023 年)[R], 2023.

[7] 中国信息通信研究院. 公共数据授权运营发展洞察(2023 年)[R], 2023.

作者简介:

王小乾 天翼云科技有限公司研发专家,高级工程师,主要研究方向为数据合规、新一代信息技术等

Risk assessment and prevention in the compliant circulation of data factors

WANG Xiaoqian

(China Telecom Cloud Computing Corporation, Beijing 100083, China)

Abstract: As a key production factor, data faces the challenge of compliant circulation in the age of digital economy. Focusing on this, this paper studies risk assessment and prevention and control measures for the compliant circulation of data factors. Although governments in China have introduced regulations such as the Data Security Law and Personal Information Protection Law to guide the compliant use of data, there are still many problems in privacy protection, data security, lagging regulations, the control of cross-border data flows, and the risks of new technologies. Therefore, this paper proposes a rigorous risk assessment scheme and gives corresponding strategies on compliance risks.

Keywords: compliant circulation; compliance risk assessment; privacy protection; compliance management system

(收稿日期:2024-01-11)