数据安全是数据要素合规发展的基石

胡亚林

武汉大数据产业发展有限公司，湖北 武汉 430023

摘　　要： 本文深入探讨了数据安全在数据要素合规发展中的核心作用。在数字化时代背景下，数据已成为关键的生产要素，对经济社会发展起到了至关重要的推动作用。概述了数据要素合规发展的概念，随后分析了数据安全的重要性，包括保障数据完整性和可用性、保护用户隐私和权益，以及促进数据共享共用和流通。文中进一步讨论了数据要素合规发展的未来展望，以及数据安全与合规发展之间的相互关系。提出了加强数据安全以促进数据要素合规发展的策略，包括法律视角下的数据安全基础、建立数据安全管理制度、加强数据加密和访问控制以及构建数据合规体系。

关 键 词： 数据安全；数据要素合规；数据治理；数据加密；访问控制

Data Security is the Cornerstone of Compliant Development of Data Elements

Hu Yalin

Wuhan Big Data Industry Development Co., Ltd. Wuhan, Hubei 430023

Abstract: This article delves into the central role of data security in the compliant development of data elements. In the digital era, data has emerged as a pivotal production factor, driving economic and societal progress. The concept of compliant development of data elements is outlined, followed by an analysis of the importance of data security, encompassing the preservation of data integrity and availability, protection of user privacy and rights, and facilitation of data sharing, collaboration, and circulation. Further discussions explore the future prospects of compliant data element development and the interplay between data security and compliant progress. Strategies to enhance data security for fostering compliant data element development are proposed, including establishing a data security foundation from a legal perspective, instituting data security management systems, strengthening data encryption and access controls, and constructing a data compliance framework.

Keywords: data security; data element compliance; data governance; data encryption; access control

引言

在数字化时代，数据已成为企业、政府和社会组织的重要资产。当前，数据以容量大、类型丰富、存取速度快、应用价值高等特征的数据集合，正快速发展为对数量巨大、来源分散、格式多样的数据进行采集、治理、存储和分析，从中发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。数据要素合规发展，即确保数据的采集、存储、治理、流通和共享共用等环节符合相关法律法规、行业准则和标准要求，对于保障数据的安全性、合法性和可靠性具有重要意义[1]。然而，随着数据规模的不断扩大和应用的不断深入，数据安全问题日益突出，给数据要素合规发展带来了巨大挑战。因此，本文将从数据安全的角度探讨数据要素合规发展的问题，并强调数据安全在其中的基石作用。

一、数据安全的重要性

（一）保障数据完整性和可用性

数据完整性和可用性的保障是数据安全的核心要素，它确保了数据在采集、存储、处理和传输过程中的准确性和一致性，防止了非法篡改和破坏。通过有效的数据安全措施，可以维护数据的原始状态，确保其随时可供授权用户访问和使用，从而支持企业的决策制定和日常运作。这种保障对于构建用户信任、促进数据共享以及推动数据驱动的创新至关重要[2]。

（二）保护用户隐私和权益

随着数字化转型的加速，个人信息的收集和使用变得日益频繁，数据泄露和滥用事件频发，对个人隐私权构成了严重威胁。数据安全措施的实施，如加密技术、访问控制和数据脱敏等，能够有效防止敏感信息的泄露，保护用户的个人隐私不被未经授权

的第三方获取或利用。强化数据安全还有助于维护用户的知情权和选择权，确保用户能够了解其数据如何被收集、使用和共享，并能够作出相应的选择[3]。这不仅有助于增强用户对企业的信任，也是企业履行社会责任、构建良好社会形象的重要途径。

（三）促进数据共享共用和流通

数据安全是促进数据共享、共用和流通的关键保障，它确保了数据在不同主体间流动时的安全性和可靠性。在当今数据驱动的经济环境中，数据的开放与共享能够激发创新，提高资源配置效率，推动社会和经济的快速发展。然而，数据共享也伴随着隐私泄露、数据滥用等风险，这就需要通过数据安全措施来降低这些风险。通过实施严格的数据访问控制、数据加密，以及对数据使用行为的监控和审计，可以在保护数据不被非法访问和滥用的同时，鼓励和促进数据的合法、合规流通[4]。

二、数据要素合规发展的展望

数据要素合规必然是数据平台合规、数据确权合规、数据治理合规、评估合规、流通合规等等。2022年12月中共中央、国务院发布了《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”），提出建立数据资源持有权、数据加工使用权、数据产品经营权的“三权分置”的数据产权制度框架。而且在《企业数据资源相关会计处理暂行规定》也强调数据资源是企业合法拥有和控制的。由此可见数据资产合规与确权是数据资产入表的首要步骤[5]。

数据要素合规是指数据所有者在数据生命周期的各个阶段，包括数据采集、存储、治理、流通、应用和销毁等环节，应遵守的法律法规、行业标准、合同约定以及内部政策等相关要求。其中，数据内容合法合规是指企业存储数据的内容需真实、合法、合规，不得存储法律法规不允许采集或存储的违法数据，如企业私自存储未依法获取授权的国家机密数据、商业秘密等；数据处理合规是指企业处理数据行为不违反国家法律相关规定，符合合法、正当、必要原则；数据安全合规是指企业采取必要的技术和管理措施，保障数据的安全性和保密性，防止数据泄露、丢失或被滥用；数据交易合规是指遵循《数据二十条》，在数据产品交易中构建合规高效、场内外一体化的数据要素流通与交易体系；数据核算合规是指数据资产入表需要遵循《企业数据资源相关会计处理暂行规定》相关要求[6]。

三、数据安全与数据要素合规的关系

（一）数据要素合规作为数据安全的前提

数据要素合规构成了数据安全的重要前提和基础。合规性要求确保数据在采集、处理、存储、传输和销毁等各个环节都遵循法律法规、行业标准和企业政策。这不仅涉及数据的质量和准确性，还包括对个人隐私的保护、数据使用的合法性以及数据访问的授权管理。数据要素合规的实施，为数据安全提供了法律和道德的框架，确保数据处理活动在法律允许的范围内进行，从而降低违规操作带来的风险。同时，数据合规还要求企业建立严格的数据治理机制，包括数据分类、数据生命周期管理、数据访问控制和数据泄露预防等策略[7]。

数据安全不仅关乎技术层面的防护，也是企业文化和价值观的体现。强化数据安全意识，培养员工对数据保护的责任感，是推动合规文化建设的重要组成部分。此外，数据安全还与企业的社会责任紧密相关，通过保护用户隐私和数据权益，企业能够建立起公众信任，提升品牌形象和社会影响力。

在全球化的背景下，数据安全合规还涉及跨国数据流动和国际合作。企业需要遵守不同国家和地区的数据保护法规，确保跨境数据传输的合法性和安全性。这要求企业不仅要有强大的技术支撑，还需要具备灵活应对不同法律环境的能力。

（二）数据安全与合规发展的相互促进

数据安全与合规发展之间存在着相互促进的良性循环关系。数据安全的高度实施不仅保障了数据的保密性、完整性和可用性，而且直接强化了企业的合规立场，使企业能够在遵守法律法规的前提下运营。反过来，强化合规性又推动企业不断完善数据安全措施，提升整体的数据治理水平。

例如，欧盟通用数据保护条例（GDPR）的实施，要求企业在处理个人数据时必须确保数据安全，同时也要遵循数据保护的原则。这促使许多企业加强了对数据访问的控制，实施了更加严格的加密措施，并改进了数据泄露的响应流程。这些改进不仅帮助企业遵守了 GDPR 的要求，也提高了它们在数据安全方面的能力，从而在全球市场中获得了更强的竞争力。此外，数据安全的最佳实践还可以作为合规发展的标杆。例如，一些企业通过获得ISO/IEC 27001信息安全管理体系的认证，展示了它们在数据安全管理方面的专业性和承诺。这种认证不仅提高了企业对内部数据管理的控制，也向外部利益相关者证明了其合规性和对数据保护的重视[8]。

四、加强数据安全促进数据要素合规发展的策略

（一）法律视角下的数据安全基础

加强数据安全以促进数据要素合规发展，首先需要从法律视角构建数据安全的基础。这包括遵循国家法律法规，如《网络安全法》《数据安全法》和《个人信息保护法》等，这些法律为企业和个人数据处理活动设定了基本规范和要求。例如，依据《数据安全法》，企业必须建立数据分类和重要数据保护制度，对数据进行风险评估，并采取相应的安全措施。

在实践中，企业可以依据这些法律法规的要求，制定和完善内部的数据安全管理制度。例如，公司可以在遵守 GDPR 的过程中，不仅对数据保护政策进行了全面修订，还加强了数据加密技术的应用，限制数据访问权限，并为员工提供了数据保护培训，以确保数据处理活动合法合规。通过这样的措施，该公司不仅提升了数据安全水平，也在全球市场中增强了用户的信任和企业的竞争力。企业还应密切关注法律法规的变化和更新，及时调整自身的数据安全策略，确保持续合规。通过法律视角下的持续

努力，企业能够在保障数据安全的同时，推动数据要素的合规发展，实现可持续发展的目标。

（二）建立数据安全管理制度

建立数据安全管理制度是确保数据要素合规发展的重要环节，它要求企业构建一套全面的安全政策和操作流程，以保障数据的安全性和合规性。例如，摩根大通银行作为全球领先的金融服务机构，其数据安全管理制度就非常严格，包括对敏感数据的加密处理、对员工进行定期的安全意识培训、实施严格的访问控制策略，以及对数据访问和使用进行持续监控[9]。这些措施帮助摩根大通银行有效预防了数据泄露事件，增强了客户对其数据保护能力的信心。此外，摩根大通还制定了详细的事件响应计划，以应对可能的数据安全事件。在2014年，尽管遭遇了一次复杂的网络攻击，但由于其数据安全管理制度的健全，摩根大通成功地限制了攻击的影响，并迅速恢复了正常运营。这一事件凸显了数据安全管理制度在实际应对安全威胁中的重要性。

通过这样的案例，可以看到，一个健全的数据安全管理制度不仅包括技术层面的安全措施，还涵盖了组织结构、人员培训、政策执行和应急响应等多个方面。这些制度的建立和执行，对于提高企业的数据安全管理水平、满足合规要求、保护客户利益以及维护企业声誉都至关重要。

（三）加强数据加密和访问控制

数据加密技术能够有效保护存储和传输中的数据不被未授权访问或泄露，而严格的访问控制机制则确保只有授权用户才能访问敏感数据。例如，美国零售巨头塔吉特（Target）在2013年遭受了一次重大的数据泄露事件，导致数百万客户的信用卡和个人数据被盗。此次事件凸显了数据加密和访问控制的重要性。随后，塔吉特投资升级了其数据安全基础设施，包括强化数据加密措施和实施更为严格的访问控制策略，以防止类似事件再次发生。

在具体实施上，企业可以采用多因素认证来增强访问控制，确保只有通过多重验证的用户才能访问敏感数据。同时，对数据进行端到端加密，即使数据在传输过程中被截获，也无法被未授权者解读。例如，苹果公司就以其强大的数据加密技术而闻名，其iOS设备提供了文件和数据的自动加密存储功能，并通过生物识别技术如Touch ID或Face ID来控制访问，确保用户数据的安全[10]。

（四）构建数据合规体系

构建数据合规体系涵盖了从数据收集、处理、存储到传输、共享和销毁的全生命周期管理，确保企业数据处理活动符合法律法规要求和行业最佳实践。例如，微软公司通过实施严格的数据合规体系，在全球范围内处理个人和企业数据时，遵循GDPR等数据保护法规。微软提供了一系列的数据保护工具和服务，如Azure Information Protection和Dynamics365，帮助客户实现数据分类、数据丢失预防和敏感数据的加密存储。

在构建数据合规体系时，企业需要制定明确的数据管理政策，包括数据分类标准、数据访问权限控制、数据保护技术要求等。同时，企业还应定期对员工进行数据保护和合规培训，增强员工的合规意识和操作技能。通过构建和维护一个全面的数据合规体系，企业不仅能够降低数据泄露和滥用的风险，还能够在数据驱动的市场中增强竞争力，赢得客户的信任和支持。真实的案例表明，数据合规体系的建立是企业数据安全管理不可或缺的一环，对于促进数据要素的合规发展至关重要。

五、结论

数据安全是确保数据要素合规发展的基石。随着数据的价值日益被认识和挖掘，其安全性问题也变得尤为突出。本文强调，企业必须从法律视角出发，建立和完善数据安全管理制度，加强数据加密和访问控制，并构建全面的数据合规体系。通过这些措施，企业不仅能够提高数据的安全性和合规性，还能够在数据驱动的市场中获得竞争优势，实现可持续发展。企业应持续关注法律法规的变化，及时调整数据安全策略，以应对不断演变的网络安全威胁。最终，企业需要将数据安全融入企业文化和运营的每一个层面，以建立公众信任并履行社会责任。

参考文献

[1] 彭星. 数字时代大数据安全防范策略的思考与研究［J］. 中国新通信，2023,25(11):88-90.

[2] 孙伟东. 基于数据安全态势背景提升企业数据安全治理能力刍议［J］. 长江信息通信，2023,36(5):168-171.

[3] 马美瑶. 企业数据合规的现实困境与实践路径［J］. 信息安全与通信保密，2022(7):150-158.

[4] 张琳琳，李晓伟. 大力开展数据安全合规性评估为数字经济发展保驾护航［J］. 信息安全与通信保密，2021(4):84-90.

[5] 黄伟庆. 合规视角下数据要素的分类分级管理机制研究［J］. 上海政法学院学报，2024,39(2):121-140.

[6] 陈名玥. App隐私政策的数据安全合规风险调查及法律对策研究［J］. 河南司法警官职业学院学报，2022,20(3):68-71.

[7] 张春艳. 大数据时代的公共安全治理［J］. 国家行政学院学报，2014（05）：100-104.

[8] 曾子明，杨倩雯. 面向第四范式的城市公共安全数据监管体系研究［J］. 情报理论与实践，2018，41（02）：82-87.

[9] 刘志坚，郭秉贵. 大数据时代公共安全保障与个人信息保护的冲突与协调［J］. 广州大学学报（社会科学版），2018，17（05）：74-79.

[10] 唐要家. 中国个人隐私数据保护的模式选择与监管体制［J］. 理论学刊，2021（1）：69-77.