

跨国企业数据合规治理挑战与措施分析

朱 意

百时美施贵宝（中国）投资有限公司 上海 200040

摘要：随着全球化进程的加速，跨国企业面临着日益复杂的数据合规治理问题。数据合规不仅是法律法规的要求，更是企业履行社会责任的重要体现。国际上许多跨国企业在数据流动治理体系中长期存在诸多问题，包括缺乏完善的数据合规治理结构，实际的可操作性不强，在数据合规方面的国际合作机制不健全而导致的信息共享推进速度缓慢，欠缺应对各国法律法规冲突的措施，以及跨国企业合规工作成本高且资源投入较大等。基于此，本文首先分析了跨国公司在数据合规治理中面临的挑战，主要包括各国数据隐私保护法规的差异、数据跨境传输的限制要求不同、以及跨国企业在数据安全保护方面的难题。其次，本文进一步探讨了实现合规的有效措施，包括建立完善的数据合规管理体系、健全数据合规监督与审计机制、以及加强数据安全保护技术手段的应用等，希望通过这些探讨，为跨国企业数据合规治理提供有价值的参考。

关键词：跨国企业；数据合规；治理难题；实现路径

引言：随着全球化的不断深入，跨国企业已经成为世界经济的重要组成部分。然而，在全球范围内进行数据管理和使用的这些企业也面临着日益增加的数据合规治理挑战。数据合规不仅是遵守法律法规的基本要求，也是企业履行社会责任的体现。不同国家和地区对数据隐私保护的法律法规差异显著，如欧盟的GDPR和美国的CCPA，这些法规要求各异，对跨国企业的数据合规治理提出了更高的要求。数据跨境传输的限制也给跨国企业的数据管理带来了挑战。例如，中国的网络安全法要求某些跨境传输的个人数据必须经过安全评估，并在中国境内存储。这对于在全球范围内运营的跨国企业来说，意味着他们在进行数据共享和业务协同时必须考虑到这些限制，增加了数据管理的复杂性。并且数据泄露和滥用的事件频发，不仅损害了消费者的利益，也严重影响了企业的声誉和财务状况。这些难题的存在，凸显了跨国企业在数据合规治理方面需要采取更为积极和有效的措施。

1 跨国企业数据合规治理挑战

1.1 数据隐私保护法规差异

跨国企业在进行数据管理和运用时，需遵循不同国家和地区的法律法规，其中数据隐私保护法规的差异性是企业面临的一大挑战。例如，欧盟的《通用数据保护条例》（GDPR）要求企业对个人数据的收集、处理和存储实施高标准保护，任何违反GDPR规定的行为都可能面临高额罚款。而美国的《加州消费者隐私法案》（CCPA）则侧重于赋予消费者对个人数据的更多控制权，并要求企业公开其数据处理方式。这两种法规在监

管范围、合规要求和处罚措施等方面都存在显著差异。

亚洲一些国家如日本和韩国，也对数据隐私保护制定了严格的法规。日本《个人情报保护法》规定了个人情报的处理原则和跨境传输的条件，而韩国的《个人信息保护法》则要求企业对个人信息的处理进行严格限制，并对数据泄露等行为进行严厉惩罚。这些法规的差异性使得跨国企业在进行数据管理和运用时，需要面对复杂的合规问题，这就需要跨国企业在数据管理中同时遵循多种法规，增加了合规难度。

1.2 数据跨境传输限制

跨国企业在数据跨境传输方面常常面临各种限制，这些限制主要来自于不同国家和地区的法律法规。例如，欧盟的《通用数据保护条例》（GDPR）对数据跨境传输设定了严格的规则，要求跨国企业在向其他国家传输欧盟居民的数据时，必须确保该传输符合GDPR的要求，并且要求企业在进行数据跨境传输之前，必须获得数据主体的明确同意，并告知其数据将被传输到其他国家。同样，美国的《加州消费者隐私法案》（CCPA）也对数据跨境传输提出了特定的合规要求，CCPA要求企业在处理本州居民的个人数据时，必须遵守严格的隐私保护标准。这些法律法规的差异性使得跨国企业在进行数据管理时面临巨大的挑战。除此之外，一些国家和地区还对数据跨境传输设定了更为严格的限制，例如要求数据在本地区本地化存储，或者在数据出境前获得相关部门的许可。这些限制对于跨国企业的全球业务运营产生了重大影响，增加了企业的运营成本和风险。以某跨国公司为例，该公司在全球范围内开展业务，需要将客户

数据从欧洲传输到亚洲的分支机构。然而,由于GDPR和CCPA等法规的限制,公司在进行数据传输时不得不采取额外的措施,如在本地区设立数据中心,以确保数据的合规性。这样的做法不仅增加了公司的运营成本,还可能影响到公司的业务效率。这些限制不仅来自于不同国家和地区的法律法规,还可能对企业的全球业务运营产生重大影响^[1]。

1.3 数据安全保护挑战

跨国企业在数据安全保护方面面临着诸多挑战,其中数据泄露和数据滥用尤为突出。数据泄露可能源于内部员工的疏忽或恶意行为,以及外部黑客的攻击。例如,在2017年,美国知名咨询公司麦肯锡(McKinsey)遭受了一次重大的数据泄露事件,内部员工的邮箱被黑客入侵,导致客户数据被泄露。而数据滥用则涉及到企业对数据的非法使用,例如,在2018年,Facebook因为剑桥分析公司(Cambridge Analytica)的数据滥用行为而受到了广泛的批评和监管机构的调查。跨国企业在数据安全保护方面还需要面对跨境数据传输的挑战。因此跨国企业如何在保证数据安全的同时满足不同国家和地区的法律法规要求,就成为企业的一大难题。

2 跨国企业数据合规治理措施分析

2.1 建立完善的数据合规管理体系

在建立完善的数据合规管理体系中,跨国企业需要考虑以下几个关键要素。组织架构的设计需确保数据合规治理的有效性。例如,设立一个由高级管理层领导的数据合规委员会,成员包括法律、IT、人力资源等部门的代表,以确保跨部门的合作和协调。职责分工明确,每名员工都应明确自己的数据合规职责和义务,例如,数据合规官负责制定和更新合规政策,监控合规情况,并处理合规事宜,进一步制定全面的数据合规制度规范是基础。这些规范应涵盖数据收集、处理、存储、传输、共享和销毁的各个环节,确保企业在任何操作中都严格遵守法律法规。例如,制定数据分类政策,根据数据敏感程度对其进行分类管理,对于高风险数据实行更严格的控制措施。操作流程的设计需要细致,包括数据访问权限的设置、数据使用记录的维护、数据泄露应急预案的制定等,都要有明确的流程和指导。合规的实现离不开内部监督和审计。企业可以设立合规审计团队,定期对各项数据处理活动进行审查,确保合规制度的执行情况,并对潜在的风险点提出改进建议。例如,对员工的数据访问记录进行审计,发现异常访问行为,及时采取措施防止数据泄露。在数据合规管理体系的建立过程中,跨国企业还应注重合规文化的培养。通过定期的

培训和宣传活动,提升员工对数据合规的认识和重视,使合规理念深入人心。例如,组织数据合规周活动,通过讲座、研讨会等形式,提高员工的数据合规意识。这一体系应包括组织架构、职责分工、制度规范、操作流程、内部监督、审计以及合规文化等多个方面,确保企业在数据管理和运用过程中,能够遵循不同国家和地区的法律法规,降低合规风险。

2.2 遵循国际标准,提升数据合规水平

在跨国企业数据合规治理的实践中,遵循国际标准被认为是提升数据合规水平的关键途径。国际标准化组织(ISO)发布的ISO/IEC 27001信息安全管理体系标准,为企业提供了一套全面的数据安全保护框架。该框架通过风险评估、物理安全、访问控制、数据加密等多个维度,确保了企业信息资产的安全。例如,某跨国科技公司在全球范围内实施ISO/IEC 27001标准,不仅使其在数据安全方面达到了国际先进水平,还成功通过了第三方认证,增强了客户对其数据服务的信任。国际数据治理委员会(DGC)制定的《全球数据治理原则》也为跨国企业提供了数据合规的指导原则,强调了数据治理的透明度、责任、公平性等核心价值。某跨国银行遵循这些原则,在全球范围内建立了统一的数据治理框架,有效协调了不同国家和地区监管要求之间的差异,提高了合规效率。通过这些国际标准的遵循和实施,跨国企业不仅能够提升自身的数据合规水平,还能在全球范围内建立起良好的合规形象,这对于获取客户的信任、降低法律风险具有重要意义。跨国企业应遵循国际数据合规标准,如ISO/IEC 27001信息安全管理体系等,提升数据合规水平。同时,企业可根据所在国家和地区的法律法规,制定针对性的合规措施^[2]。

2.3 加强数据合规培训与宣传

在跨国企业的数据合规治理中,加强数据合规培训与宣传是提升全员合规意识、深化合规文化的重要措施。培训与宣传的内容应深入浅出,将复杂的法律法规转化为易于理解的实践指导,确保每一位员工都能认识到自己在数据保护中的角色和责任。例如,可以组织针对性的研讨会,邀请法律专家解读《通用数据保护条例》(GDPR)或《加州消费者隐私法案》(CCPA)的关键条款,并结合企业实际情况,说明遵循这些法规的具体要求和操作流程。在案例方面,可以引用真实的企业违规事件进行分析。比如,某跨国公司在某一地区因未能遵守当地数据保护法规而遭受重罚,这样的案例能够生动地说明合规的重要性。还可以分享企业在数据合规方面的良好实践,如某公司的数据泄露应急预案演

练,通过模拟演练让员工了解在数据安全事件发生时如何迅速响应和处理,增强实操能力。宣传方面,企业可以利用内部通讯、海报、在线课程等多种形式,持续性地传达数据合规的信息。例如,制作简洁明了的数据保护宣传册,放置在办公区域的公共区域,或通过企业内部网络平台,发布数据保护小贴士,提醒员工在日常工作中注意数据合规。通过这样系统化、多样化的培训与宣传,可以有效地提升跨国企业员工的数据合规意识,促进企业形成良好的数据合规文化,从而在全球化背景下确保企业的稳健运营和法律责任的履行。

2.4 建立健全数据合规监督与审计机制

跨国企业在面对数据合规治理的挑战时,建立健全数据合规监督与审计机制至关重要。这一机制旨在确保企业遵循不同国家和地区的法律法规,并有效应对数据安全保护的挑战。具体而言,企业应定期对数据合规工作进行检查和评估,以识别潜在的风险和问题。企业可设立数据合规审计团队,负责对数据合规制度执行情况进行监督。审计团队应具备专业知识和经验,能够对企业数据合规工作进行全面、深入的评估。通过建立健全的数据合规监督与审计机制,跨国企业可以提高数据合规水平,降低合规风险,确保数据的合法、合规使用。

2.5 加强数据安全保护技术手段的应用

随着信息技术的飞速发展,数据加密、访问控制等安全技术不断涌现,跨国公司需要有效运用数据安全技术手段,来增加企业数据的保护工作,而数据加密技术是保护数据安全的重要手段。通过将敏感数据进行加密处理,即使数据被非法获取,也无法被轻易解读。访问控制技术也是保障数据安全的关键。通过设置权限和身份验证,确保只有经过授权的用户才能访问敏感数据。例如,某跨国公司采用了基于角色的访问控制(RBAC)系统,根据员工的工作职责和权限,动态地控制其对数据的访问。数据安全保护技术还包括数据脱敏、安全审计等。数据脱敏技术可以将敏感数据进行变形处理,使其在分析和挖掘过程中不再具有原始数据的特点,从而保护个人隐私。安全审计技术则可以帮助企业监控和分

析系统的安全状况,及时发现并应对潜在的安全威胁。然而,在实际应用中,跨国企业仍面临诸多挑战。例如,如何合理地配置加密算法和访问控制策略,以实现数据安全与业务效率的平衡;如何应对不断变化的安全威胁,及时更新和优化安全技术;如何确保安全技术的实施和维护,以避免人为疏忽导致的数据安全问题等。因此只有通过采用先进的数据加密、访问控制、数据脱敏和安全审计等技术,企业可以有效保障数据安全,降低数据泄露和滥用的风险^[3]。

结论

跨国企业在面对全球化进程中的数据合规治理挑战时,需认识到数据隐私保护法规差异、数据跨境传输限制和数据安全保护挑战等难题。这些难题不仅源于不同国家和地区法律法规的差异,还体现在数据传输的限制和安全保护的挑战上。针对这些难题,跨国企业应采取一系列措施以实现数据合规治理。首先是建立完善的数据合规管理体系。其次需要遵循国际标准,如ISO/IEC 27001信息安全管理体系,有助于提升数据合规水平。再次,加强数据合规培训与宣传也是实现数据合规治理的关键。跨国企业可以通过定期举办数据合规培训和研讨会,提高了员工对数据合规的认识和重视,使得数据合规理念深入人心。最后,企业还需要加强数据安全保护技术手段的应用。跨国企业可以通过采用数据加密和访问控制等技术手段,确保了数据的安全性。针对数据泄露等安全事件,企业需要制定应急预案,以降低安全风险。通过这些措施,跨国企业能够有效应对数据合规治理挑战,确保合规经营。

参考文献

- [1]冷竹星.跨国企业数据合规治理难题与实现路径[J].时代经贸,2023,20(09):82-85.DOI:10.19463/j.cnki.sdjm.2023.09.029.
- [2]韩露.跨国长产业链企业中财务BP的数字化转型——以S公司为例[J].国际商务财会,2024,(05):77-82.
- [3]陈兵,徐文.数据跨境流动的治理体系建构[J].中国特色社会主义研究,2021(04):67-75.