企业数据保护和应用合规思路探讨

贾淑琴

（上海市企业法律顾问协会，上海　200070）

摘要：本文探讨了企业数据保护和应用合规的策略。首先强调了数据保护和应用合规的重要性，突出它们在保护敏感信息和降低法律风险方面的作用。讨论了对数据保护的理解，包括定义和法律框架，以及确保应用合规的关键要素。企业数据保护的策略涵盖了风险评估、数据分类、加密、访问控制和用户认证等方面。应用合规措施的实施包括面向隐私的设计原则、定期审计、数据泄露应对和培训计划等。强调持续评估和改进对于保持数据保护和合规工作的有效性至关重要。总结起来，企业必须优先考虑数据保护、合规性和适应性，以维护隐私权利并与利益相关者建立信任关系。

关键词：企业数据保护；应用合规；网络威胁

中图分类号：C931.2；TP3　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2023.26.015

在当今数字时代，数据的快速增长和对技术的日益依赖为企业带来了许多益处。然而，这种数据生成和利用的指数级增长也引发了人们对于敏感信息保护和合规要求遵守的担忧。数据保护和应用合规的重要性已成为各个行业企业的首要任务。数据保护涉及保护敏感信息免受未经授权的访问、使用、披露、篡改或破坏。它包括实施安全措施、政策和实践，以确保数据的保密性、完整性和可用性。随着网络威胁、数据泄露和隐私问题的增加，企业必须优先考虑强大的数据保护机制，以维护利益相关者的信任、遵守法律义务，并降低潜在的财务、法律和声誉风险。

与数据保护并行的应用合规是指遵守适用的法律法规和标准，以管理软件应用程序的开发、部署和使用。它涵盖了数据隐私、同意管理、信息安全和伦理等多个方面。实现应用合规对企业至关重要，以展示它们对负责任的数据处理实践的承诺，保护个人权利，并保持合规性[1]。

1 理解数据保护

1.1 数据保护的定义和意义

数据保护是指为了防止数据未经授权的访问、使用、披露、篡改或破坏而采取的一系列实践、政策和措施。它涵盖了一系列活动，旨在在数据的整个生命周期中确保数据的机密性、完整性和可用性。数据保护的重要性在于它作为企业信息安全、隐私保护和风险管理的基本要素。有效的数据保护措施对于维护个人隐私和信任至关重要，这些个人的数据被企业收集、处理和存储。通过保护敏感信息，企业可以防止未经授权的披露、滥用或利用，从而维护数据主体的权利和期望，此外，数据保护措施可以减轻数据泄露的风险，而数据泄露可能对企业造成严重的财务、法律和声誉影响。

1.2 与数据保护相关的法律和监管框架

（1）国家和国际法律

数据保护受到一系列国家和国际法律的管理，这些法律确立了与个人和敏感数据处理相关的法律义务和权利。各个国家或地区的数据保护相关法律，如欧洲联盟的《通用数据保护条例》（GDPR）、美国加州的《加州消费者隐私法》（CCPA）以及中国的个人信息保护法、网络安全法、数据安全法等法律法规，为数据和隐私保护制定了一系列的框架和要求，概述了数据控制者和处理者在处理与此有关事务时应遵守的原则和要求、权利和义务等[2]。

在国际层面上，像《保护个人关于自动处理个人数据的公约》和亚太经济合作企业（APEC）隐私框架这样的框架提供了跨境数据保护的一些指导和标准，此外，跨境数据转移机制，如欧盟－美国隐私盾框架和标准合同条款，对于个人数据在这些不同司法管辖区之间的合法转移也进行了相关规定。

（2）行业特定的法规

除了一般的数据保护法律，某些行业还有特定的法规，针对其行业内的独特数据保护要求进行规范。例如，美国的医疗保险可移植性和责任法案（HIPAA）规定了医疗行业对医疗记录和患者个人身份信息的保护。同样，金融行业也遵守《支付卡行业数据安全标准》（PCI DSS）等法规，以确保信用卡信息的安全处理。

行业特定的法规通常概述了行业内特定的数据保护标准、数据保留期限、数据泄露通知要求和合规框架，以满足各行业内的独特风险和考虑因素。对于在这些行业运营的企业来说，遵守这些法规是至关重要的，可以减轻风险，保持消费者信任，并避免法律和财务处罚。了解围绕数据保护的法律和监管框架对企业至关重要。遵守适用的法律要求，确保企业履行法律义务，并满足数据主体、监管机构和利益相关者的期望和要求。通过遵守这些框架，企业可以有效保护数据，降低风险，并与客户和合作伙伴建立起信任的基础。

2 确保应用合规

2.1 应用合规概述

应用合规是指企业在与数据有关的软件应用程序在开发、部署和使用过程中遵守适用的法律法规和标准。它涵盖了确保应用程序符合法律法规、监管要求、数据安全和隐私保护以及同意管理等方面。应用合规对企业来说至关重要，可以展示其对负责任的数据处理实践的承诺，保护个人数据安全和隐私权利并确保合法合规性。

2.2 合规要求和标准

（1）通用数据保护法规

应用合规的基础是通用数据保护法规，它为企业制定了基本框架。例如，欧盟的《通用数据保护条例》（GDPR）和中国的《中华人民共和国个人信息保护法》规定了其管辖范围内的有关个人数据的合法处理原则和要求，包括获得有效同意、赋予个人数据权利以及采取适当的技术和企业措施确保数据安全等。在适用上述 GDPR 或个人信息保护法的司法管辖区内运营的企业应当严格遵守相关规定，以保护个人的隐私权利，并避免不合规的严厉处罚。

（2）行业特定的合规指南或管理指南

除了上述比较通用的数据保护法规以外，许多行业还制定了自己行业的特定合规指南或管理指南，以满足其特定要求。例如，美国的医疗保险可移植性和责任法案（HIPAA）规定了医疗保健行业对受保护的健康信息（PHI）的安全处理要求，要求实施严格的管理、技术和物理安全措施，以保护患者的隐私和机密性。例如，中国的《汽车数据安全管理若干规定（试行）》专门针对汽车行业的数据安全管理作了特别规定。这些专门针对特定行业的数据合规指南或管理指南，更为清楚地针对该特定行业的独特数据保护、安全和隐私问题作出了特别规定。

2.3 应用合规面临的挑战

确保应用合规面临一系列挑战，企业必须在复杂的法律和监管环境中谨慎操作。其中一个重要挑战是法律和法规的不断变化，需要不断监测和调整以使应用程序符合新的合规要求。企业必须保持警觉并积极主动，及时了解新的法规、行业指南和最佳实践，以确保持续合规并减少潜在风险。不遵守应用规定和标准对企业会产生严重的影响。从法律角度来看，违反数据安全和隐私保护法律可能面临巨额罚款、处罚和制裁。非合规行为的财务影响不仅限于法规罚款，还可能涉及法律纠纷、客户赔偿要求和业务运营中断，此外，不合规行为对企业的声誉产生负面影响，破坏客户信任并导致负面公众认知。企业的品牌形象和市场地位受损可能难以挽回，通常需要大量投资来重建信任和可信度。

不遵守应用规定可能会增加企业面临的网络安全风险和数据泄露风险，进一步引发法律问题和企业声誉的受损。如果未能实施强大的安全措施、有效的同意管理协议或充分的数据保留政策，就可能导致未经授权访问、滥用或丢失敏感信息，给个人和企业带来严重伤害。数据泄露的连锁效应可能影响企业的声誉，损害客户关系，并引发连锁的财务和法律后果。

3 企业数据保护的策略

3.1 风险评估与管理

一个有效的企业数据保护策略的重要组成部分是进行全面的数据安全和隐私保护风险评估并实施有效的风险管理措施。风险评估的过程包括识别、分析和评估可能对企业数据安全和机密性构成威胁的潜在漏洞、威胁和风险。通过评估这些风险的概率和潜在影响，企业可以全面了解其数据环境，并根据潜在风险的严重性和可能性确定保护措施的优先级，此外，风险管理策略使企业能够制定和实施适当的控制措施、安全防护和缓解策略，以降低风险和漏洞。这包括建立事故响应计划、灾难恢复协议和业务连续性措施，以确保数据保护机制在遇到突发事件发生时的弹性和可持续性，避免因此类数据泄露或突发事件而导致业务中断或损失。通过积极管理风险，企业可以有效保护其宝贵的数据资产，并维护利益相关者的信任。

3.2 数据分类和加密等技术措施

企业数据保护的基本支柱之一是实施数据分类和加密措施。数据分类涉及根据其敏感性、机密性和法规要求对数据进行分类。通过为不同类型的数据分配分类标签或元数据，企业可以有效识别和区分不同敏感性级别的数据，如个人敏感信息、企业商业保密信息、国家核心数据或重要数据。此分类使企业能够根据每个数据类别的特定要求应用适当的安全控制和加密方法。另一方面，加密是一种强大的技术，通过使用密码算法将数据转换为不可读格式，以确保其机密性和完整性。通过加密数据，企业可以确保在未经授权的访问或数据泄露的情况下保持数据的机密性。加密在数据传输或存储过程中尤为重要，它提供了额外的保护层，防止数据被截获或未经授权披露。除了加密之外，企业还可以采取例如匿名化、去标识化、身份鉴别、访问控制等技术措施，以尽量避免 / 减少数据被非法损毁、丢失、篡改或未经授权地披露或访问。综上，实施健全的数据分类和加密实践有助于企业开展数据安全和隐私保护，从而减轻与数据泄露和未经授权访问相关的风险 [3]。

3.3 访问控制和用户认证

要加强企业数据保护，企业必须实施严格的访问控制措施并实施强大的用户身份验证协议。访问控制涉及建立机制以规范和控制用户对敏感数据和资源的访问。它涵盖了各种策略，如基于角色的访问控制（RBAC），根据职位角色和责任授予访问权限，并执行最小必要原则，确保用户仅具备执行任务所需的最小数据和系统访问权限，此外，实施强大的用户身份验证机制对验证寻求访问系统或数据的个人的身份至关重要。该身份验证过程可能涉及密码、生物识别、多因素身份验证或其他

高级身份验证技术。通过强制实施访问控制和用户身份验证措施，企业可以显著降低未经授权访问、数据泄露和内部威胁的风险。这些措施为未经授权的个人试图访问敏感数据提供了额外的防护层，从而保护企业信息的机密性和完整性。

成功实施这些策略需要综合方法，其中包括技术措施、内部制度和政策以及持续地员工培训计划。企业应定期评估和更新其数据保护策略，以适应不断发展的威胁、技术进步和法规要求，此外，培养员工对数据保护的意识和责任文化对于这些策略的有效实施至关重要。通过推动和营造关于数据安全和隐私保护的企业文化，在企业的行为准则和道德伦理中融入数据安全和隐私保护意识，员工将成为帮助保护数据安全、减少漏洞并应对潜在数据漏洞或安全事件的积极参与者。

4 实施应用合规措施

4.1 隐私设计原则

在企业数据保护和应用合规的背景下，“面向和保护隐私的设计”概念起着至关重要的作用。面向和保护隐私的设计是指在应用程序、系统和流程的整个生命周期中积极整合隐私考虑和保护措施的做法。它涉及从初始设计阶段就嵌入隐私控制和措施，确保在应用程序的开发、部署和运行过程中考虑并实施隐私要求。通过融入面向和保护隐私的设计原则，企业可以尽量管理和规避数据隐私风险，加强数据保护，并展示对维护隐私权利和法规的承诺。这包括实施增强隐私的技术、进行隐私影响评估，并采用诸如数据收集和提供时的最小必要化原则、目的限制和透明度等面向和保护隐私的做法。面向和保护隐私的设计原则为应用合规提供了坚实的基础，使企业能够将其日常实践与隐私法律和法规保持一致。

4.2 定期审计和监控

为确保持续符合数据保护法规和标准，企业必须建立定期的审计和监控机制。定期审计使企业能够评估其应用合规措施的有效性，识别漏洞或不足，并采取纠正措施。审计涉及审查和检查现行的流程、控制和程序，以确保其与适用的法规和行业最佳实践保持一致。这包括评估数据收集、使用、委托处理、对外提供、转移、存储和处理等事项的准确性和完整性，以及评估安全措施和访问控制的有效性。除了审计，持续监控对于实时检测和解决任何合规问题至关重要。通过实施强大的审计和监控实践，企业可以保持对应用合规的积极态度，识别漏洞或改进领域，并及时解决可能出现的合规问题。

4.3 数据泄露通知和应对

为应对潜在的数据泄露或安全事件，企业应当制定明确的流程和程序，以有效处理在发生该类突发事件时的应急处理。数据泄露通知和应对措施涉及及时透明地与受影响个人、监管机构和其他相关利益相关者进行沟通。企业应及时评估泄露的数据性质、范围和程度，及时采取措施避免或减轻进一步的损害，并采取适当措施来恢复和保护受影响的数据。这包括向受影响个人通知泄露事件、提供防护措施指南，并与监管机构依法进行汇报或接受查询或调查。此外，企业应制定对于该等突发事件的应对计划，以及明确关键人员的角色和责任，及时和妥善开展相关沟通，并采取措施尽快遏制和解决问题以及尽快恢复正常运营。通过实施有效的应对措施，企业可以展示其对保护个人隐私权利的承诺，最小化泄露的影响，并遵守法律义务。

4.4 培训计划

有效实施数据保护和应用合规措施依赖于员工的知识和意识。企业应投资开展全面有效的培训和意识培养，以帮助员工了解和掌握有关数据保护法规、隐私要求以及认真履行他们在确保合规方面的角色和责任。培训计划应涵盖数据处理实践、安全编码技术、隐私影响评估和事件报告程序等主题。通过推广数据保护和隐私意识文化，企业可以为员工赋能，提升员工做出明智决策、识别潜在数据合规风险和遵守最佳实践的能力。持续的培训活动和计划还可以帮助企业及时了解不断变化的合规要求和新兴问题，确保员工具备必要的技能和知识，以保护企业的数据安全并保持应用合规性[4]。

5 结语

数据保护领域不断发展，新技术不断涌现，新的挑战和潜在风险也在不断演变，法规环境也在不断变化。因此，企业必须采取积极主动的方法，及时了解这些变化，并确保其数据保护和合规工作的有效性。持续评估使企业能够识别需要改进的领域，解决漏洞，并将其实践与最新的法规要求保持一致。此外，通过培养持续改进的文化，企业应建立一个能及时适应各种变化的、能有效开展数据安全和隐私保护的坚实合规框架。企业必须优先考虑持续评估和改进数据保护和合规措施，以便有效管理和降低潜在风险，履行企业对于保护数据安全和遵守相关法规的承诺，获得企业客户、供应商等外部合作伙伴的认可和信任，并有效维护企业的良好声誉。

参考文献：

[1]陈锋，曹忠明．企业数据保护与隐私合规策略探讨．现代信息[J]．2017，34（02），73-76．

[2]张丽华，刘伟．大数据环境下企业数据保护与合规问题研究．电子科技导报[J]．2016，14（03），67-71．

[3]曾鹏，刘东芳．基于大数据的企业数据保护与合规策略研究．现代信息技术[J]．2018，48（08），161-164．

[4]杨宁，杨雪梅，林琳．企业数据隐私保护合规性问题研究．电子技术应用[J]．2019，45（05），11-15．

作者简介：贾淑琴（1975-），女，江苏南通人，硕士研究生，主要从事外商投资、合规等研究。