

数据隐私保护对企业合规管理的影响

陈白冰

新疆丝路互连数字产业发展有限公司，新疆 乌鲁木齐 830011

DOI:10.61369/SE.2025050008

摘 要： 本研究将立足于数据隐私保护的主体，以企业管理为核心切入基点，集中分析当前相关工作中所存在的主要问题，深入阐述工作改革所具有的核心意义，分别立足于完善合规制度、加强员工培训、建立风险评估机制、强化第三方管理等角度提出若干策略性建议，希望能够助力企业在数据隐私保护与合规管理间达成更为理想的平衡状态，继而实现其自身的可持续发展目标。

关 键 词： 数据隐私保护；企业；合规管理；意义；问题；策略

The Impact of Data Privacy Protection on Enterprise Compliance Management

Chen Baibing

Xinjiang Silk Road Interconnection Digital Industry Development Co., LTD., Urumqi, Xinjiang 830011

Abstract： This research will focus on the theme of data privacy protection, taking enterprise management as the core entry point, and intensively analyze the main problems existing in the current related work. It will deeply elaborate on the core significance of work reform and put forward several strategic suggestions from the perspectives of improving compliance systems, strengthening employee training, establishing risk assessment mechanisms, and enhancing third-party management. It is hoped that this can help enterprises achieve a more ideal balance between data privacy protection and compliance management, and thereby realize their own sustainable development goals.

Keywords： data privacy protection; enterprise; compliance management; meaning; problem; strategy

引言

在信息技术飞速发展的高维视域下，数据开始被广泛应用于各个企业的运营环节体系当中，以客户关系管理、市场营销、产品研发、供应链管理为代表的环节更是表现出了巨大的数据流量。与此同时，各企业在数据隐私保护方面也开始面临诸多挑战，数据泄露事件层出不穷，给企业和用户都带来了十分严重的损失。在数据保护法规日益严格的总体形式下，企业如果不能有效地采取措施保护数据隐私，必然会面临巨大的法律风险和声誉损害。因此，广大企业务必要投入更多的资源去研究、完善数据隐私保护的思路和策略，继而确保企业能够实现合规管理并服务于后续的长效发展。

一、数据隐私保护对企业合规管理的重要意义

（一）避免法律风险，确保企业合法运营

全球关于数据保护方面的法律建设日臻完善，针对企业数据收集、存储、使用、共享和删除等行为提出的要求也日趋严格、明确。根据 GDPR 相关规定，企业若在相关领域出现违规操作，最高可能被处以全球年营业额 4% 或 2000 万欧元（取其高者）的罚款；而我国的《个人信息保护法》也进一步明确了对违规企业的警告、罚款、停业整顿等处罚措施。因此通过进一步重视、完善数据隐私保护工作，企业可以更为严格地遵循法规要求，继而有效避免因违规操作而造成的法律风险，保障自身的合法、优化运营。

（二）增强客户信任，提升企业声誉

在信息时代的大背景下，客户对自身的个人数据隐私普遍报以高度的关注。如果企业可以更为妥善地保护客户的数据隐私，便可让其更为放心地提交个人信息，从而增强客户对企业的信任感，在强化客户黏性的同时维护、优化企业的业绩和社会声誉——从这一角度出发来看，数据隐私保护是企业赢得客户信任、提升声誉、扩大市场份额的关键性保障因素之一。

（三）保护企业核心资产，提升竞争力

从本质层面上来看，数据可以被看作是企业的核心资产，以商业机密、客户数据、运营数据等为代表的键数据对企业的决策、创新和市场竞争等活动都起着至关重要的作用。通过保护数据隐私，企业可以进一步防止数据泄露的出现，有效避免

竞争对手获取关键信息并维持企业自身的竞争优势，确保企业的核心技术研发数据、市场管理数据和关键客户信息得到安全利用，使其得以在市场竞争中凭借自身的独特优势脱颖而出^[1]。

二、企业在数据隐私保护方面存在的合规问题

通过之前的调查不难发现，目前一些企业对数据保护方面的法律法规还没有形成足够深入的认识，继而导致其在实际的运营活动中经常出现一些违规行为。譬如，部分企业对 GDPR 中有关“用户数据访问权、更正权和删除权”方面的规定不甚了解，没有及时响应用户提出的相关请求，继而面临巨大的法律风险。此外，很多国家、地区在数据保护方面的具体法律规定还存在着巨大差异，而部分企业在跨国业务并没有精准了解、有效满足对应的法规要求，致使自己在涉外业务中因合规难度大而出现不必要的失误。

除此之外，一些企业内部的数据管理工作暴露出混乱问题，数据的存储较为分散，缺乏足够统一的数据分类以及权限管理机制。这一现象的存在容易导致企业员工对数据访问权限无法形成明确意识，继而出现诸如数据滥用、泄露等方面的风险。另外，还有一些企业在数据安全技术研发、引入投入不足，网络防护能力十分薄弱，难以有效抵御可能发生的黑客攻击，导致自身数据泄露事件频发。

还需提及的一点是，不少企业在运营活动中经常与云计算服务商、外包商等第三方合作伙伴共享核心数据，而如果其对第三方数据的安全监管工作不到位，也非常容易引发一系列的数据隐私风险。在这一方面，部分企业对于第三方合作伙伴的选择过于草率，没有充分评估其在数据安全方面的能力、信誉，同时未在合同中进一步明确数据安全方面的责任，导致第三方出现数据泄露问题时使自身也受到了法律、经济和社会声誉层面的牵连性损失。

三、企业应对数据隐私保护合规管理的策略

（一）完善企业数据隐私保护合规制度

“无有规矩，不成方圆”，只有建立、健全对应的工作规章制度，相关工作的执行才能够做到有章可循、有法可依。立足于此，企业务必要同步结合国内外有关数据保护方面的法律法规以及自身的业务项目、规模、服务群体等特质来制定更加全面、详细的数据隐私保护政策及具体的工作流程，以标准化的模式来明确数据的收集、存储、使用、共享、删除等各项关键环节的操作规范以及责任主体，并对违规操作行为制定足够严格的惩戒措施，同时设立数据隐私风险发生时的应急预案和常规管理台账，从而在最大程度上确保数据处理活动能够得到有力的制度框架保障^[2]。

例如，对于互联网运营层面的业务活动，企业应当在基本管理制度的基础上出台更具针对性的数据隐私保护政策，详细规定用户注册时数据收集的“最小必要”原则，进一步明确相关单位、个人仅收集被直接用于服务设计、完善的姓名、联系方式等

关键信息，避免因过度收集而导致的数据隐私泄露风险；与此同时，企业还要建立、健全对应的数据分级分类管理制度，具体针对用户数据的敏感程度来进行不同的等级建设，将客户的身份证号、银行卡号等直接涉及个人信息、经济权益的数据列为高敏感数据，并要对不同等级的数据采取对应的安全防护措施，对高敏感数据要采用多重加密存储保障，相关的靶向访问活动需要经过更加严格的审批流程。在条件满足时，企业还要定期对合规制度进行阶段性审查和更新，从而确保其与国家法律法规的变化以及企业自身业务的调整保持高度一致。

（二）加强员工数据隐私保护意识培训

人才是企业所掌握的核心资源，也是推进工作优化开展的第一驱动。在数据隐私保护方面，企业要投入大量资源开展人才培训活动，定期组织员工——尤其是信息数据管理部门的员工参加对应主题的数据隐私保护培训课程，积极联系、邀请相关方面的法律专家及安全技术人员主持授课，课程的内容要同步涵盖数据保护法规解读、企业内部数据隐私政策讲解以及安全操作规范培训等核心项目，同时还要结合本企业或行业内其他企业的真实案例分析来引导员工更为深刻地认识数据隐私保护的重要性以及违规操作所造成的严重后果。此外，企业还可积极发动员工进行数据隐私保护方面的自主学习和技术自研工作，将相关领域的人才培养活动拓展到员工的个体层面，进一步强化工作的综合推进、优化内驱力^[3]。

比如，企业可以定期邀请当地律师事务所负责信息安全领域的律师来为信息管理部门员工做主题培训，讲解我国出台的关于数据隐私保护方面的详细法律条文，就数据保护的 legal 意识、社会意义以及违法后果等做具体阐述；还可引入行业内企业因员工疏忽导致数据泄露进而使企业遭受巨大损失的案例做具象讲解，使员工能够在直观层面上感受到数据安全的重大意义和责任。在讲解和案例解析结束后，企业要组织员工参与主题培训考核，将数据隐私保护方面的知识作为考核核心，同时将考核的结果与员工个人的绩效挂钩，继而激励员工们更为积极开展自主学习活动。

（三）建立数据隐私风险评估与应急响应机制

“防患于未然”是所有风险应对工作的核心思想。企业应当进一步重视对数据隐私风险的综合评估以及应对应急响应机制的设立、优化工作，在开展新的数据处理活动之前要建立全体系的风险评估模型，重点围绕新产品用户数据收集、第三方共享大量数据建设等重点项目做模块评估，集中分析相关业务活动可能存在的数据隐私风险、用户数据被滥用风险等隐私风险，对风险等级做出量化表达并形成复合性的分析体系，同时结合分析体系结果来制定与之相应的应对措施，以此来在数据隐私保护领域形成全域度的安全覆盖网络。在这一同时，企业还要制定更加详细的数据泄露应急响应预案，明确数据泄露发生时各部门、人员的具体职责和对应的处理流程，在数据泄露事件发生后第一时间启动预案并采取通知用户、向监管部门报告、配合调查等措施控制事态发展^[4]。

例如，对于涉及用户个人经济活动方面的服务项目，企业应

先通过 DPIA 来做模拟分析,通过“大数据”插件和虚拟沙盘软件做多场景解析,发现相关数据在传输过程中最容易存在被黑客截取等类型的安全隐患,而后便可对此采取“用户数据以加密形式传输”以及“增加身份认证环节”等措施来及时降低风险指数。而当数据信息出现泄漏问题后,企业要责令客户对接部分迅速通知受影响的客户并详细告知其可能会面临的风险及对应的防范措施,同时向监管部门报告事件的发生情况并积极配合调查;此外,企业还要结合 DPIA 在阶段内的分析结果定期对应急响应机制进行靶向演练、优化工作,进一步提高应对数据泄露事件的质量和效率,通过模拟不同场景的数据泄露事件,检验应急响应流程的合理性和有效性并及时发现、改进问题和措施,继而确保在实际发生数据泄露时能够快速、有效地应对。

(四) 强化对第三方合作伙伴的数据安全管理

企业在经济活动中必然要与第三方机构频繁开展合作,而这也无形中增加了数据隐私泄露等方面的风险。立足于此,企业在选择第三方合作伙伴前应当率先对其数据安全方面的能力进行体系性的评估,重点关注其安全技术水平、数据管理体系、过往数据安全记录等项目,同时还要结合第三方机构的数据安全领域法律纠纷历史做必要调查。在涉及核心项目活动时,企业还应要求第三方提供 ISO 27001 信息安全管理体系认证等相关安全认证证书,进一步了解其在数据安全方面的资源投入和保障措施体系建设情况。在这一系列工作的基础上,企业还要定期对第三方合作伙伴的数据安全状况进行监督和审计,同时要求其提供数据安全方面的活动报告,以此来确保其能够严格遵守合同约定并履行数据保护法规中的义务^[5]。

例如,企业在选择云服务提供商时应当对多家候选供应商进行综合性的评估,同步采取现场考察、问卷调查等不同路径来了解其数据中心所采取的安全防护措施、数据备份策略,并以复合

型的评价模型为机制来确定数据安全能力强、信誉良好的供应商。在后续与第三方签订的合同中,企业要详细明确双方在数据安全方面的责任和义务,重点突出数据保护标准、数据访问权限、数据泄露赔偿责任等核心项目,规定第三方不得将企业数据用于合同约定之外的其他用途,同时对发生数据泄露时双方应承担的法律责任和经济赔偿做具体要求。如果企业发现第三方存在数据安全方面存在问题,应当及时根据业务诉求和法律法规要求其整改,若整改不力则要第一时间终止合作关系,在更高层面上确保数据安全。

除了以上几个方面的主要策略外,企业还要将数据隐私安全保护工作融入企业文化、氛围的营造当中,定期以团建、文艺联欢、主题座谈会等活动形式和企业文化墙、企业官网、微信公众号等载体形式宣传数据隐私保护方面的法律规定、行业责任及典型案例,真正让相关工作的开展结果在员工群体中“入心入脑”,为其他方面工作的优化开展奠定必要的“软基础”。

四、结束语

总而言之,数据隐私保护对企业合规管理至关重要,直接关系到企业的生存与发展。广大企业责任人员务必要通过完善合规制度、加强员工培训、建立风险评估与应急响应机制以及强化第三方管理等策略来构建对应的保障机制,有效应对数据隐私保护中的合规挑战,在合法合规的前提下充分挖掘数据价值,从而大大增强企业的生命力和竞争力。随着数据保护法规不断完善和技术的持续发展,企业还要持续关注数据隐私保护方面的动态并不断优化合规管理措施,以此来更好地适应日益复杂的数据安全环境,继而实现企业的可持续发展。

参考文献

- [1] 舒蓉. 数据隐私保护与合规性要求在企业人事档案管理中的重要性 [J]. 时代人物, 2024(8): 33-35.
- [2] 谢佰刚. 数据隐私法律框架下的企业责任与合规管理研究 [J]. 法制博览, 2024(19): 142-144.
- [3] 张琛. 国有企业物资线上采购业务数据隐私保护方法研究 [J]. 技术与市场, 2024, 31(12): 38-42, 47.
- [4] 晏海水, 王亚军, 廖璇. 数字化时代企业合规管理的关键挑战与技术驱动的对策 [J]. 现代企业文化, 2024(36): 58-60.
- [5] 陶海敏. 大数据时代的隐私保护和信息安全管理 [J]. 山西电子技术, 2024, (06): 71-72+109.