E-Commerce Letters 电子商务评论, 2025, 14(5), 3348-3356
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.1451647

Hans汉斯

ERP系统中的客户关系管理与数据保护法律分析

张贵珍

贵州大学法学院，贵州 贵阳

收稿日期：2025年4月11日；录用日期：2025年4月26日；发布日期：2025年5月31日

摘 要

随着信息技术的不断发展，企业资源规划(ERP)系统成为了企业管理的核心工具，尤其是在客户关系管理(CRM)方面，得到了广泛的应用。ERP系统通过整合客户数据、销售记录、客户需求等信息，帮助企业提升客户满意度并优化业务流程。然而，随着数据保护法规的日益严格，企业在使用ERP系统进行客户关系管理时，如何合法、合规地处理客户数据，尤其是个人数据，成为了一个急需解决的问题。本文将分析ERP系统中客户关系管理(CRM)与数据保护的法律问题，探讨在现代法律框架下如何平衡企业数据需求和客户隐私保护，最终提出相关的法律规制建议。

关键词

ERP系统，客户关系管理，数据保护，法律规制，隐私保护

Legal Analysis of Customer Relationship Management and Data Protection in ERP Systems

Guizhen Zhang

Law School of Guizhou University, Guizhou Guiyang

Received: Apr. 11th, 2025; accepted: Apr. 26th, 2025; published: May 31st, 2025

Abstract

With the continuous development of information technology, enterprise resource planning (ERP) system has become the core tool of enterprise management, especially in customer relationship management (CRM), which has been widely used. ERP systems help enterprises improve customer

文章引用: 张贵珍. ERP 系统中的客户关系管理与数据保护法律分析[J]. 电子商务评论, 2025, 14(5): 3348-3356.
DOI: 10.12677/ecl.2025.1451647

satisfaction and optimize business processes by integrating customer data, sales records, customer needs and other information. However, with the increasingly stringent data protection regulations, how to legally and compliantly handle customer data, especially personal data, when enterprises use ERP systems for customer relationship management, has become an urgent problem to solve. This article will analyze the legal issues of customer relationship management (CRM) and data protection in ERP systems, discuss how to balance enterprise data needs and customer privacy protection under the modern legal framework, and finally put forward relevant legal regulatory recommendations.

Keywords

ERP System, Customer Relationship Management, Data Protection, Legal Regulation, Privacy Protection

1. 引言

近年来，全球各国纷纷出台或完善个人信息保护法律，以规范企业对客户数据的收集、存储、使用和共享。例如，欧盟的《通用数据保护条例》(General Data Protection Regulation, GDPR)、中国的《个人信息保护法》(PIPL)、美国的《加州消费者隐私法案》(CCPA)等法律法规，都对数据主体的权利、企业的数据处理责任、数据跨境传输规则等作出了严格规定。这些法律的出台对 ERP 系统中的 CRM 模块带来了深远影响，要求企业在使用 CRM 系统进行客户数据管理时，必须符合相关法律要求，否则将面临法律责任甚至高额罚款。

因此，在企业纷纷引入 ERP 系统、加强客户关系管理的同时，如何在提升客户体验的同时保障客户隐私、确保数据的合法合规处理，已成为企业管理者、法律从业者及政策制定者必须深入研究和解决的重要问题。

2. ERP 系统中的客户关系管理与数据保护法律框架

2.1. ERP 系统的功能与 CRM 模块的重要性

在全球数字化转型的推动下，企业资源规划(Enterprise Resource Planning, ERP)系统已经成为现代企业管理的重要工具。ERP 系统的核心价值在于整合企业内部资源，提高运营效率，优化决策流程[1]。它是一种集成化管理软件，旨在通过一体化的技术平台，帮助企业整合内部各个职能部门的资源与信息，以提高企业的整体管理效率。ERP 系统涵盖了从采购、生产、销售、库存管理到财务、人力资源等各个领域，通过统一的数据存储和流通平台，确保企业资源的最佳配置。简单来说，ERP 系统是一个以客户为中心、以时间为基础、覆盖整个供应链管理的企业资源规划体系[2]。客户关系管理(Customer Relationship Management, CRM)作为 ERP 系统的关键组成部分，承担着客户数据管理、市场分析、客户服务优化等多项职能。一般认为销售、市场营销和客户服务是 CRM 的三大功能支柱[3]。通过 CRM 模块，企业能够有效收集、存储并分析客户信息，从而制定精准的营销策略，提升客户忠诚度和市场竞争力，虽然这提升了企业的市场竞争力，但同时也引发了一系列法律与合规问题，特别是在数据保护与隐私权方面。客户关系管理(CRM)是现代企业管理中的一项重要战略，旨在通过高效的管理手段建立和维持企业与客户之

间的长期、稳定的关系。CRM 是一种商业管理策略，它通过使企业组织、工作流程、技术支持和客户服务都以客户为中心来协调和统一与客户的交互行动，达到保留有价值客户，挖掘潜在客户，赢得客户忠诚，并最终获得客户长期价值的目的[4]。

在信息技术快速发展的背景下，ERP 系统的功能逐渐扩展，尤其在客户关系管理(CRM)模块的加入后，系统功能更加完善和多元化。ERP 系统中的 CRM 模块，主要用于管理与客户相关的所有信息，涵盖客户数据收集、客户需求分析、销售预测、市场活动管理、客户支持与售后服务等。通过这种信息集成和自动化管理，企业能够实时了解客户需求，预测市场趋势，优化服务质量，并通过精准营销提升客户满意度与忠诚度。

在竞争日益激烈的市场环境中，企业若想保持持续的竞争力，必须高度重视客户关系管理。传统的“交易型”市场已经转向更加注重客户体验的“关系型”市场，客户的需求和偏好愈加多样化，企业需要不断优化与客户的互动，满足个性化需求。通过 ERP 系统中的 CRM 模块，企业能够实时获取客户的个人信息、购买记录、需求偏好等数据，从而进行精准营销和客户维护，提高客户满意度，并建立强大的客户忠诚度。

然而，尽管 ERP 系统中的 CRM 模块提供了许多便利和优势，如何在管理和利用客户数据时保持合法合规，尤其是在个人数据保护和隐私安全方面，仍然是当前企业面临的一大挑战。企业需要在高效管理客户关系的同时，确保遵守数据保护相关法规，避免数据泄露和隐私侵犯。

2.2. 客户数据的收集、处理与管理模式

在 ERP 系统中，客户关系管理(CRM)模块的核心功能之一便是客户数据的收集与管理。企业通过 CRM 系统收集各类客户信息，包括基本的个人信息(如姓名、联系方式、地址等)、购买历史、客户反馈、客户行为记录等。这些数据为企业提供了客户画像，帮助企业了解客户需求、购买偏好和潜在市场趋势[5]。

随着数据采集技术的发展，企业对客户数据的获取不仅局限于直接的交易记录，还涉及客户在社交平台上的行为数据、网络浏览记录、移动设备位置数据等多方面的内容。大数据和人工智能技术的引入，使得企业能够在极短的时间内分析出客户的消费习惯、兴趣偏好和潜在需求。这些信息为企业的精准营销、产品推荐和客户服务提供了极大的便利。

然而，客户数据的收集和管理也伴随着一定的法律风险，特别是在数据量越来越庞大的情况下，企业必须严格遵守相关法律规定，确保数据收集与使用不侵犯消费者的隐私权。例如，收集敏感信息如个人身份证号、银行卡信息等时，企业必须明确告知客户其数据收集的目的、使用范围以及存储期限，并且在法律允许的框架内获取客户的明确同意。

一旦客户数据被收集，如何使用这些数据来提升企业运营效率并保护客户隐私，便成为了企业面临的重要问题。在 ERP 系统中，客户数据的处理通常分为以下几个步骤：

(1) 数据存储与整理：企业首先将收集到的客户数据进行存储和整理。数据应保存在安全的环境中，采用加密、访问控制等技术手段确保数据的安全性。

(2) 数据分析与挖掘：企业可以通过数据分析技术，深入挖掘客户的消费习惯、购买偏好等信息，生成客户画像。基于这些分析结果，企业可以制定精准的市场营销策略，如个性化推荐、定向广告等。

(3) 数据共享与协作：为了提升业务协作，部分企业可能会将客户数据共享给其他部门(如销售、客服等)，或通过数据共享平台与合作伙伴进行协作。这时，数据的使用权限和范围应明确界定，以避免滥用客户数据。

(4) 数据销毁与删除：根据法律规定，企业在客户请求时应提供数据删除服务。特别是在客户停止使

用服务或要求删除其个人数据时，企业必须及时履行数据删除的义务。

2.3. 法律框架与数据保护要求分析

随着数据隐私问题的日益严重，全球范围内的各国政府和国际组织逐步加强了对个人数据保护的立法。对于企业而言，确保客户数据的合法使用是至关重要的。对于 ERP 系统中客户数据的管理，最为关键的法律规定通常涉及以下几个方面：

(1) 数据收集与同意：根据数据保护法规(如 GDPR，《个人信息保护法》)，企业在收集客户数据时必须获得客户的明确同意[6]。客户应被告知其数据将如何使用，如何存储，以及是否会与第三方共享。企业还应提供客户选择退出或删除数据的选项。

(2) 数据存储与安全：企业需要采取适当的技术和组织措施，确保客户数据不被未经授权的人员访问或篡改。数据存储和管理平台应符合安全标准，如加密技术、访问控制、数据备份等，以降低数据泄露的风险。

(3) 数据处理与透明度：客户有权知晓其个人数据的使用方式，包括其数据如何被分析、存储以及是否会被转移给第三方。企业必须定期更新隐私政策，确保客户能够获得准确、清晰的信息。

(4) 数据访问与删除：客户应当有权访问其个人数据，查看数据是否准确、是否有误。同时，客户有权要求企业删除其个人数据，特别是在客户停止使用相关服务或撤销同意的情况下。企业必须建立透明的流程，以便客户能够行使这些权利。

在这一过程中，企业如果未能合规地处理客户数据，不仅可能面临来自监管机构的处罚，还可能因为数据泄露或不当使用而遭遇客户诉讼。比如，2018 年 GDPR 的实施让欧盟企业面临着高额的罚款和监管压力，全球范围内的企业也不得不加强数据隐私保护。

在信息化的时代，企业通过 ERP 系统收集和处理大量客户数据，如何在技术创新与法律合规之间找到平衡，成为了现代企业需要解决的重要问题。为了确保企业在客户数据的处理过程中合法合规，全球范围内多个国家和地区相继出台了各类数据保护法律及条例，为数据管理与隐私保护提供了法律依据。

《欧盟通用数据保护条例》(GDPR)：GDPR 于 2018 年 5 月生效，成为全球数据隐私保护领域的标杆。其核心要求是确保个人数据的收集、存储、处理、使用及传输都必须在合法、透明、明确的框架下进行。企业在使用 ERP 系统时，必须确保客户数据的采集是基于明确的同意，且仅限于特定的、合法的目的。此外，GDPR 还规定了数据主体(即客户)的多项权利，包括访问权、修正权、删除权、数据转移权等，企业必须为客户提供相应的机制来行使这些权利。在数据转移问题上，GDPR 提出了数据跨境的一般原则，任何正在处理或打算在转移给第三国或国际组织后处理的个人数据的转移，包括从第三国或国际组织向另一个第三国或另一国际组织转发个人数据，管理者和处理者都应遵守一定的条件，以保证自然人不受损害[7]。

《个人信息保护法》：2021 年实施的《个人信息保护法》进一步提升了中国在数据隐私保护方面的法律水平，尤其对企业数据处理行为提出了具体的合规要求。根据《个人信息保护法》，企业必须明确告知消费者数据的采集目的、处理方式以及存储期限，且客户同意的取得必须具备主动性。在数据存储方面，该法律要求企业加强数据安全措施，防止数据泄露和滥用，尤其是涉及个人敏感信息时，应采取加密、匿名化等措施进行保护。

《加利福尼亚消费者隐私法案》(CCPA)：CCPA 适用于加利福尼亚州内的所有企业，它更多聚焦隐私数据本身，以个人信息使用的效率与边界为切入，重点关注个人信息处理分析及第三方披露开放利用等情形的主体知悉权、充分选择及授权，以充分披露和主体授权为前提允许数据控制企业为商业目的披露或向第三方共享开放隐私数据[8]。虽然 CCPA 在美国尚未形成统一的全国性法律，但它在数据保护方

面的严格要求对 ERP 系统中的客户数据处理具有重要指导作用。

这些法律为企业在使用 ERP 系统处理客户数据时提供了框架，并明确规定了企业在数据收集、存储、使用和删除等方面的责任和义务。

2.4. 数据保护的基本原则与合规性要求

在 ERP 系统中，企业处理客户数据时需要遵守一系列数据保护的基本原则。通过明确这些原则，企业可以有效减少合规风险，并确保在数据管理中的透明度和合法性。

(1) 合法性、公正性和透明性：企业必须确保客户数据的收集和使用具有法律依据。根据相关法律，数据收集必须基于客户的明确同意，且使用目的必须是合法和正当的。此外，企业应向客户明确告知其数据将如何使用、存储、传输及共享，确保客户对数据处理的透明知情。

(2) 目的限制：客户数据只能用于明确、合法且合理的目的。企业在使用 ERP 系统收集客户数据时，必须确保数据的收集不超出原定目的，避免数据滥用。例如，收集客户信息时，企业必须确保仅用于销售、营销或服务优化等合理目的，而非用于其他未经授权的活动。

(3) 数据最小化：企业在使用 ERP 系统时，应仅收集与实现业务目标相关的最低限度数据[9]。比如，在进行市场分析时，企业应仅收集与客户行为相关的必要数据，而不是将所有可能收集到的个人数据全部存储和使用。

(4) 数据准确性：确保客户数据的准确性是企业合规义务的重要方面。ERP 系统中存储的客户信息必须准确、更新，并及时更正过时或错误的数据。客户有权要求查看和修改其个人信息，企业应提供便捷的方式让客户进行数据纠正。

(5) 存储期限：根据《个人信息保护法》和 GDPR，企业在存储客户数据时，应遵循“存储期限最短原则”，即仅在达成目的所必需的时间内保留数据。一旦数据的存储目的达成，企业应及时删除或匿名化数据，以防止不必要的风险。

(6) 数据安全性：企业必须采取必要的技术和组织措施，确保客户数据不被未授权的人员访问、泄露或篡改。在 ERP 系统中，企业应使用加密技术、访问控制、数据备份等手段保护数据安全。此外，企业还应进行定期的安全检查，及时发现并解决潜在的安全漏洞。

2.5. 企业合规性管理体系的建设

为了确保 ERP 系统中客户数据的处理符合相关法律法规要求，企业需要建立健全的数据保护管理体系。具体来说，企业可以从以下几个方面着手：

(1) 数据保护官(DPO)的设立：根据 GDPR 的要求，某些类型的企业需要任命数据保护官(DPO)。数据保护官在任内需要承担的任务包括：通知与建议任务、监督任务、与监管机构配合执行其他任务等[10]。即使企业不需要正式任命 DPO，也应有专门的团队负责数据合规和保护工作。

(2) 合规审计与风险评估：企业应定期进行数据保护审计和风险评估，以识别和解决潜在的合规风险。在 ERP 系统的实施过程中，企业需要评估其系统中的数据流动和处理过程，确保所有数据处理活动都符合合法、公平和透明的原则。此外，企业应确保对数据的访问与使用权限进行严格管理，防止员工滥用权限，确保数据不被非法获取或篡改。

(3) 数据保护培训与意识提升：企业必须定期为员工提供数据保护相关的培训，增强员工对数据保护法规和企业数据处理政策的认识。培训内容应包括如何收集、存储、使用和传输客户数据，如何确保数据安全，如何应对数据泄露等突发事件。同时，企业应倡导数据保护文化，让每个员工都能积极参与到数据保护的工作中。

(4) 客户数据管理平台的合规性设计：在 ERP 系统的设计和实施过程中，企业应与技术供应商密切合作，确保系统本身具备强大的数据保护功能。例如，系统应具备加密、身份验证、权限管理等安全模块，确保数据处理符合各国法律法规的要求。

3. ERP 系统中客户数据保护面临的挑战

3.1. 数据跨境流动的合规性问题

随着全球化进程的加速，许多企业采用跨境 ERP 系统，客户数据经常需要在不同国家和地区之间流动。这就引发了数据跨境传输的合规性问题。根据《个人信息保护法》和 GDPR 的规定，个人数据的跨境传输必须满足严格的合规要求。例如，GDPR 要求在跨境传输数据时，企业必须确保接收方国家或地区具备足够的数据保护水平，或者通过签订数据保护协议(如标准合同条款)来确保数据的安全性[11]。根据 Kuner (2013)在《国际数据保护法》中的研究，数据主权与跨境流动的冲突本质上是国家数字治理权的博弈[12]。《个人信息保护法》和 GDPR 虽已建立基本框架，但各国对“充分保护水平”的认定差异显著。例如，欧盟法院在 Schrems II 案中否定了欧美“隐私盾协议”，导致企业不得不采用更复杂的标准合同条款(SCCs)。这种法律冲突不仅增加合规成本，更迫使企业建立动态的合规监测机制，以应对不同法域的数据本地化存储要求。在现实中，如何确保数据跨境流动不违反当地的数据保护规定，成为企业的一大难题。

3.2. 技术与法律的脱节

技术的快速发展，特别是大数据、人工智能、区块链等技术的应用，使得数据的处理和利用方式发生了根本性变化。以个性化定价算法为例，现行《反垄断法》仅规制价格同盟等传统行为，对基于客户数据的动态歧视定价缺乏认定标准。区块链技术的不可篡改性虽然增强审计能力，但其分布式存储特征却与 GDPR“被遗忘权”产生根本冲突。这种脱节在 ERP 系统整合新技术时尤为突出，企业往往陷入技术创新合规与法律解释不确定性的双重困境。然而，现有的数据保护法律大多滞后于技术发展[13]。例如，算法歧视、个性化定价等新兴问题在技术上得到了广泛应用，但现有的法律框架尚未对这些技术的使用进行明确规制。ERP 系统作为企业信息管理的重要工具，其在处理客户数据时，可能存在对新技术应用的法律适应性不足，导致法律空白和监管难题。

3.3. 企业合规性意识的不足

统一合规意识薄弱本质上是成本收益错配问题。ERP 系统实施中常见的认知偏差包括：将 ISO27001 认证等同于法律合规，忽视数据分类分级的具体要求；误判“合法必要原则”的适用边界，过度采集客户设备指纹等生物特征数据。更严重的是，很多企业尚未建立数据保护官(DPO)制度，导致合规决策缺乏专业支撑。尽管在全球范围内已有多个数据保护法规出台，但许多企业尤其是中小型企业对数据保护法律的认知仍存在一定盲区。尤其是在 ERP 系统的实施和管理过程中，企业往往将重点放在技术实施和效率优化上，而忽视了数据保护的法律合规性。合规就是企业要遵守经营活动所在地的法律法规，确保企业的经济活动符合“公共利益”[14]。因此，缺乏系统的法律培训和合规意识，可能导致企业在客户数据处理过程中不小心违反相关法律法规，面临法律风险和经济损失。

3.4. 数据泄露和内部安全管理问题

ERP 系统中存储大量敏感数据，如客户个人信息、交易记录等，一旦出现数据泄露，可能对客户和企业带来巨大的损失。在实际操作中，数据泄露往往源于企业内部的管理漏洞或员工操作不当，而不是

外部黑客攻击。例如，员工对数据访问权限管理不当，或者企业未能及时修补系统漏洞，都会导致客户数据泄露。如何加强内部数据安全管理，防止员工滥用数据访问权限，成为保护客户隐私的重要问题。ERP 系统特有的风险点在于：销售模块与 HR 模块的权限交叉可能使普通业务员获取客户身份证号等敏感字段；工作流审批日志的留存缺失导致溯源困难。这要求企业必须建立细粒度访问控制(ABAC)体系，并实施基于用户行为的实时异常检测。

4. ERP 系统中客户数据保护的合规策略

为应对上述挑战，企业需要采取一系列的对策来提升 ERP 系统中客户数据保护的合规性，确保在满足法律要求的前提下进行高效的数据管理和客户关系维护。

4.1. 建立跨境数据流动的全流程管控

在 ERP 系统中涉及到跨境数据传输时，企业必须确保遵守相关国家和地区的数据保护法律。企业应当与国际合作伙伴及数据传输方建立数据合规合作机制，共同确保数据传输过程中不发生数据泄露或滥用问题。针对跨国企业数据跨境传输难题，建议从业务源头开始建立数据流向地图。首先在 ERP 系统部署初期，就应当明确识别所有可能涉及数据跨境的功能模块，例如跨国子公司间的库存共享、全球客户服务中心的数据调取等场景。对于向欧盟地区传输数据的情况，企业需要确保满足 GDPR 对跨境数据传输的要求，采取相应的法律保障措施，如签订标准合同条款或使用欧盟认证的第三方数据处理服务商。除此之外，还可以在系统中设置双重确认机制——当操作人员试图导出包含客户个人信息的数据包时，系统会自动弹出法律风险提示，并需要至少两名管理员授权才能执行。同时建议企业定期(至少每季度)更新跨境传输白名单，将业务需求减少的国家地区及时移出传输范围，从源头降低合规压力。

4.2. 优化数据安全防护的技术组合

为了增强客户数据的安全性，企业应当在 ERP 系统中使用先进的加密技术，确保数据传输和存储过程中的安全性。通过数据加密，可以有效防止数据被黑客窃取或泄露。同时，企业可以考虑使用数据匿名化技术，尤其是在分析客户行为和交易记录时，通过匿名化处理，使数据不再直接关联到个人，从而减少数据泄露的风险和潜在的隐私侵害。

在技术防护层面，需要采取分层防御策略。对于存储环节，建议对客户基本信息(如姓名、电话)采用基础加密保护，而对敏感信息(如身份证号、银行账户)则实施增强加密，即使发生数据泄露也能最大限度降低信息可用性。在数据分析场景中，可以建立“数据脱敏工作区”，当业务人员需要使用客户数据进行市场分析时，系统自动替换关键字段，例如将真实电话号码替换为虚拟号码，将具体年龄转换为年龄段(如 25~30 岁)。此外，建议在 ERP 系统设置自动化巡检功能，每周自动检测加密密钥有效期、访问日志完整性等核心安全指标。

4.3. 开展靶向式员工能力培养

企业应当定期为员工特别是数据处理部门的员工提供数据保护法律和合规性培训，确保每一位员工都能明确自身在数据保护中的责任和义务。特别是 IT 部门和 ERP 系统管理员，应当清楚如何设置和管理系统中的数据访问权限，确保客户数据不被未经授权的人员访问和篡改。要使全员牢固树立依法治企的理念，通过培训进一步提高全员的民主意识和法律素养，以符合市场经济规律和一流企业的要求[15]。

人员培训需要突破传统模式，建议采用“场景化教学 + 实战演练”相结合的方式。对于新入职员工，在初次登录 ERP 系统时强制完成 20 分钟交互式培训，通过模拟客户数据泄露事故的动画演示，直观展示错误操作可能引发的法律后果。针对关键岗位人员(如销售主管、财务专员)，每季度组织沉浸式演练：

设置虚构客户数据违规场景(如擅自导出客户名单参加展会)，要求参与人员在 30 分钟内完成风险识别、应急处置等全流程操作。同时建议建立培训效果追踪机制，将员工在 ERP 系统中的实际操作合规率(如二次认证使用频次、日志填报完整度)与绩效考核挂钩。此外，还应定期进行内部合规性检查，及时发现潜在的合规问题，进行修正和改进。

4.4. 构建数据权限管理机制与应急响应体系

企业应当制定详细的数据处理和存储政策，对客户数据的采集、存储、使用、删除等各个环节进行规范。政策中应明确规定客户数据的存储时间，以及数据在使用完毕后的销毁方式。为了遵守数据保护法律的要求，企业还应在 ERP 系统中设置数据过期自动删除功能，确保不再使用的数据及时删除或匿名化。企业需要建立覆盖事前预防、事中监控、事后响应的完整管理体系。在日常运营阶段，建议为每个 ERP 功能模块定制安全检查清单，例如采购模块重点监控供应商数据共享范围，客服模块则着重审查通话录音存储周期。在系统访问控制方面，可实施动态权限管理：当员工调岗至不涉及客户数据的部门时，其原有数据访问权限应在 24 小时内自动降级。对于突发数据安全事件，建议设立三级响应机制：普通事件(如单个客户信息误发)由部门安全员 2 小时内处理；重大事件(如批量数据异常下载)需立即启动跨部门工作组；危机事件(如黑客入侵数据库)则直接由总经理组建应急指挥部。

尽管企业已经采取了严格的数据保护措施，但在数据泄露或安全事件发生时，企业仍需快速反应。为此，企业应建立完善的数据安全应急响应机制，确保在数据泄露事件发生时，能够迅速定位问题源、评估风险，并采取补救措施。根据 GDPR 的规定，企业在发生数据泄露时，必须在 72 小时内向监管机构报告，必要时还应通知受影响的客户[16]。因此，企业应提前制定应急预案，确保在事件发生时能够快速响应，降低损害和法律责任。

5. 结语

随着数字经济的深入发展，企业对客户数据的依赖程度日益加深，ERP 系统与客户关系管理(CRM)的融合不仅提高了企业运营效率，也带来了更高的数据风险与法律挑战。本文通过分析 ERP 系统中客户数据采集、处理、使用等环节中的主要法律问题，尤其是在数据跨境、技术适应、企业合规意识及内部安全管理等方面，揭示了当前企业面临的多重挑战。

针对这些问题，本文提出了相应的法律与制度对策，强调企业应构建完善的合规管理体系、强化数据加密与匿名化技术的使用、制定明确的数据处理规范，并在客户关系管理中实现隐私保护与业务发展的平衡。这些对策不仅有助于提升企业合规水平，也为企业在全球数据合规趋势下稳健运营提供了参考。

当然，本文仍存在一定不足，如未涉及具体企业案例，数据处理技术与法规适配方面也缺乏实证验证。未来研究可进一步结合行业实践，对不同类型企业的合规策略进行实证分析，或从 AI、大数据背景下的数据权利重构角度深入探讨数据保护制度的演进方向。

参考文献

[1] Davenport, T.H. and Harris, J.G. (2013) Competing on Analytics: The New Science of Winning Davenport. *Journal of Information Technology Case and Application Research*, **15**, 59-61. https://doi.org/10.1080/15228053.2013.10845729

[2] 苏博, 李惠娇, 管冬河. 数智化背景下 ERP 系统的发展机遇与挑战研究[J]. 现代信息科技, 2024, 8(23): 138-144.

[3] 傅翀, 唐小我. ERP 与 CRM 的发展趋势分析[J]. 电子科技大学学报(社科版), 2001, 3(3): 72-75.

[4] 齐佳音, 李怀祖. 客户关系管理(CRM)的体系框架分析[J]. 工业工程, 2002, 5(1): 42-45.

[5] Zikopoulos, P. and Eaton, C. (2011) Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. McGraw-Hill Osborne Media.

[6] Jančiūtė, L. (2019) European Data Protection Board: A Nascent EU Agency or an 'Intergovernmental Club'?

International Data Privacy Law, **10**, 57-75. https://doi.org/10.1093/idpl/ipz021

[7] 吴沈括, 霍文新. 欧盟 GDPR 与数据跨境问题分析[J]. 中国信息安全, 2018(7): 31-33, 37.

[8] 陈慧慧. 比较视角看 CCPA 的立法导向和借鉴意义[J]. 信息安全与通信保密, 2019(12): 26-36.

[9] 梅傲, 苏建维. 欧盟数据最小化原则研究[J]. 国别和区域研究, 2024(1): 64-83, 310.

[10] 王楠. GDPR “数据保护官”制度探析——兼论其对中国的启示[J]. 电子知识产权, 2019(6): 16-26.

[11] Schwartz, P.M. and Solove, D.J. (2011) The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *NYU Law Review*, **86**, 1814.

[12] Kuner, C. (2013) Transborder Data Flows and Data Privacy Law. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

[13] 陶乾, 宋春雨. 企业数据泄露的法律治理困境与规范适用[J]. 中国信息安全, 2021(5): 34-36.

[14] 王志乐. 强化合规经营意识促进企业持续发展[J]. 新产经, 2018(9): 14-16.

[15] 董薇薇, 李明霞, 陶富莲. 企业合规管理与培训的针对性分析[J]. 人才资源开发, 2015(8): 78.

[16] 郑令晗. GDPR 中数据控制者的立法解读和经验探讨[J]. 图书馆论坛, 2019, 39(3): 147-153.