数字化时代下的企业合规：隐私保护和数据安全的法律视角

崔雅怡
广东金轮律师事务所，广东　广州　510515

摘要：在数字化时代，企业面临着日益增长的数据量和不断变化的技术环境。同时，个人信息的泄露和数据安全问题也成为当今社会关注的焦点。本文将从法律视角探讨数字化时代下企业合规中的隐私保护和数据安全问题，并提出相关的解决方案。通过分析现行法律框架、审视企业责任以及了解个人权利，可以为企业提供合规建议，帮助其更好地保护用户隐私并确保数据安全。

关键词：数字化时代；隐私保护；数据安全

随着科技的迅速发展，数字化已经渗透到了各行各业。企业借助数字技术来提升效率、创新产品和服务，以期与消费者建立更紧密的联系。随之而来的是企业留存的海量数据的保存、使用，以及个人隐私保护的问题。如何在数字化时代中确保企业数据合规，成为一项紧迫的任务。

一、数字化时代下的隐私保护法律框架

不同国家和地区制定了各种不同的隐私保护法律，以应对日益增长的数字化世界中涉及个人信息的风险和挑战。这些法律旨在保护个人的隐私权利，并要求企业在收集、存储和处理个人信息时遵守一系列规范和标准。

例如，欧盟的《通用数据保护条例》（General Data Protection Regulation，GDPR）是当前最为严格和综合的隐私保护法律之一。规定了个人数据的收集、使用和转移的条件，强调了个人对于其数据的控制权，并要求企业提供透明和清晰的隐私政策。此外，GDPR 还规定了违反隐私规定可能导致的高额罚款，以确保企业严格遵守法律的要求。

而加拿大则制定了《个人信息保护与电子文件交易法》（The personal Information Protection and Electronic Documents Act，PIPEDA），该法律旨在保护个人敏感信息的隐私和安全。要求企业获得个人信息的有效同意，并限制了个人信息的收集和使用范围。此外，PIPEDA 还规定了个人信息泄露后的通知和报告要求，以确保个人在信息安全方面得到适当的保护[1]。

除了这些国际性的法律框架之外，许多国家和地区还制定了自己的隐私保护法律，以适应本地的特定需求和环境。这些法律通常涵盖了数据保护、信息安全、数据主体权利等方面的内容，并设立了监管机构来监督和执行法律的实施。

我国关于隐私保护的法律规定正处于快速发展阶段，制定了一系列相关法律法规，包括《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）等，这些法律法规为数据合规提供了法律依据和指导。其中，《个人信息保护法》规定了个人信息的收集、使用、存储、传输和删除的具体规定，鼓励企业加强个人信息保护，同时对个人信息泄露行为制定了严格的惩罚措施。

总体来说，我国的隐私保护制度发展情况正在稳步提升，随着法律法规的完善和社会的普及，隐私保护意识在政府和企业中不断增强，中国正朝着更加合规、安全的隐私保护方向迈进。

二、企业在数字化时代下的责任

在数字化时代，企业面临着维护用户隐私和数据安全的重要责任。为了履行这一责任，企业需要采取一系列措施来保护用户信息并应对潜在的安全威胁。

企业应该加强内部管理，并建立完善的数据保护机制。这包括对敏感信息进行分类和权限管理，确保只有经过授权的人员才可以访问和处理这些信息。通过建立严格的数据访问控制和审计机制，企业可以有效地防止未经授权的数据泄露和滥用。企业需要经常进行风险评估，及时发现和应对潜在的数据安全威胁。这意味着企业应该密切关注最新的网络安全信息和数据泄露事件，并采取相应的预防和应急措施。企业可以提高自身的网络安全防御能力，通过加强企业数据安全等级，提升安全技术水平，实时进行安全漏洞扫

描、加强加密技术和增加安全监控工具，减少潜在的安全风险。企业还应该加强员工培训，提高员工对隐私保护和数据安全的意识。通过定期的培训和教育活动，企业可以帮助员工了解最新的安全威胁、防范措施和违法责任，并教育他们如何正确处理和保护用户的个人信息[2]。

三、数字化时代下需强化对个人隐私权利的保障

在数字化时代，强化对个人隐私权利的保障是至关重要的。个人拥有保护自己隐私的权利，这意味着企业在收集个人信息时需要遵守一定的规定和原则，企业在收集个人信息之前必须事先征得个人的明确同意。

在这个过程中，意味着个人在接受企业提供的服务或与企业做交易时，必须事先知道企业对他们的信息进行收集的行为，并且有权选择是否同意。企业应当提供清晰、易懂的告知文件，明确说明信息的用途和范围。在收集过程中，个人有权决定是否愿意分享自己的信息，分享哪些信息，还享有访问、更正和删除个人信息的权利。而企业则有责任尊重个人的选择，在业务的范畴内有限度地收集相关信息。这意味着个人有权了解企业持有哪些与自己相关的信息，并有能力对其中的错误或过时信息进行更正或修改；如果个人决定撤回先前的同意或不再希望企业继续持有其信息，也有权要求企业删除这些信息。

企业应该建立相应的机制来保障个人权利的实施，并及时响应个人的请求。企业应该尊重个人权利，并采取措施来保护个人信息的安全。这包括采取合理的技术和组织措施，以防止未经授权的访问、使用或泄露个人信息。企业还应该明确相应的隐私政策，向个人说明其信息的处理方式，并为个人提供修改、变更、删除及投诉的渠道。

四、确保企业在数字化时代下合规的措施

（一）遵守法律法规

企业需要深入研究当地的隐私保护法律法规，确保自身行为符合相关规定。隐私保护法律法规的遵守不仅可以帮助企业建立良好的信誉，还可以保护个人信息的安全。

在现代社会中，个人信息的泄露已经成为一个严重的问题。因此，各国纷纷出台了相关的隐私保护法律法规，以保护公民的个人信息安全。企业作为信息的收集和处理者，有责任确保其所采集的个人信息的安全性，避免因个人信息的泄露产生违法责任。

企业应该了解当地的隐私保护法律法规，并且按照当地的法律法规的要求制定措施。第一，企业应该提高员工关于个人隐私保护的法律意识，了解隐私保护的重要性，并且严格按照企业指定的保护措施执行操作；第二，企业应该建立健全的内部隐私保护制度，包括明确的数据收集和处理流程、安全的存储和传输方式，以及相关个人信息的访问权限和使用范围等；第三，企业还应该进行定期的内部审核和风险评估，确保隐私保护工作的有效性。

在全球化的背景下，企业可能需要面对来自不同国家或地区的数据传输和处理要求，除了遵守当地的隐私保护法律法规之外，企业还应该关注国际上的隐私保护标准，如数据涉及跨境传输，则相关企业需要了解相关数据涉及的国家、地区法律法规的规定，并制定符合相关地区法律法规要求的操作流程，以确保数据符合每一个涉及地区或国家的数据安全要求。

（二）加强内部管理

企业在保护个人信息安全方面，除了遵守法律法规外，还需要加强内部管理。建立和完善企业内部数据保护和隐私保护的规章制度是加强内部管理的重要一环，该机制应当包括敏感信息的分类和权限管理，以防止未经授权的访问和使用。企业应该对所收集到的个人信息进行合理分类。根据信息的敏感程度和风险等级，将其划分为不同的类别。例如，个人身份证号码、银行账号等属于高风险敏感信息，而姓名、地址等则可能属于低风险敏感信息。通过对信息进行分类，企业可以更好地对高风险敏感信息提供特别保护和控制。同时，企业应该采取适当的权限管理措施，确保只有经过授权的人员才能访问和使用敏感信息。权限管理可以通过建立严格的访问控制机制来实现，包括用户身份验证、分配不同级别的权限、限制对敏感信息的访问等。此外，企业还应该定期审查和更新权限，以适应组织内部变化和员工职责的调整[3]。

（三）进行风险评估

为了保护个人信息的安全，企业需要及时发现和应对潜在的数据安全威胁。为此，进行风险评估是至关重要的步骤，可以帮助企业识别可能存在的风险，并采取相应的措施进行风险管理。

企业可以定期通过系统性的风险评估来识别潜在的数据安全威胁，包括对企业内部的数据收集、存储、处理和传输过程进行全面的分析和评估。通过细致审查和评估，企业可以识别出可能存在的数据泄露、未经授权访问、网络攻击等风险事件。

同时，企业还应该考虑外部因素，及时关注法律法规和行业标准的变化，更新和调整企业

的隐私保护措施，确保与时俱进。企业应该制定相应的风险管理策略和措施。根据风险评估的结果，企业可以确定哪些风险是最紧迫和严重的，对应地制定应对方案及建立紧急响应计划，以应对发生数据安全事件时的紧急情况。进行风险评估不能仅仅停留在一次性的工作上，而应该是一个持续的过程。随着技术和威胁的不断演变，风险评估也需要不断更新和完善。

因此，企业应该定期进行风险评估，并根据评估结果及时调整和改进相应的措施和策略，改进数据安全措施、加强网络防御、建立灵活的数据备份和恢复机制等以保证个人信息的安全。

（四）加强培训

对企业的员工加强培训，是提高企业在隐私保护方面的合规认识及风险意识的重要方法。这些培训可以涵盖以下内容：向员工介绍相关的法律法规、行业标准和公司政策，确保他们了解并遵守隐私保护和数据安全的法规和要求；教育员工如何识别潜在的隐私和数据安全风险，并提供应对策略，以帮助他们避免和应对各种安全威胁；详细介绍员工在处理个人数据时需要遵守的最佳实践和流程，包括数据收集、存储、传输和删除等方面的操作；加强员工对于敏感信息（如个人身份信息、财务信息等）的保护意识，强调保密性、完整性和可用性的重要性；培训员工在发生数据安全事件或安全漏洞时的应急响应流程，以确保他们能够快速、有效地应对可能的威胁。

（五）精细化管理个人信息

企业在保护隐私方面，应当确保对于个人信息的收集、使用、存储和删除符合相关法律法规的要求，明确告知信息主体对其个人信息处理的目的、方式和范围，并经过信息主体的明示同意。比如：要求企业或员工需在获得用户明确的同意时才开始收集用户个人信息，并向用户说明收集信息的目的和使用方式；通过技术设计，严格规定内部员工对于个人信息的访问权限和使用限制，建立严格的访问控制机制，仅允许授权人员在必要情况下访问和使用个人信息；采取加密、防火墙、反病毒软件、安全审计和漏洞扫描等安全措施来保护个人信息的安全性；严格控制个人信息与第三方共享的条件，并在必要时制定数据转移的规范；如信息需要用于共享的情况下，应当确保与第三方合作伙伴签订合适的协议，以保护个人信息的安全和隐私；对于违反隐私保护和数据安全政策的员工进行纪律处罚，并建立举报渠道，鼓励员工积极报告任何违规行为。

（六）进行第三方审核和认证

为了增加透明度和可信度，委托独立的第三方机构对企业的隐私保护和数据安全措施进行定期的审核和认证。这些第三方机构将负责评估企业的合规性、数据安全性和隐私保护措施的有效性。

通过审查企业的隐私保护和数据安全政策，以确保其符合相关法律法规和行业标准。他们将核实企业是否遵守了数据保护原则，并对企业的数据处理流程进行评估。第三方机构将评估企业采取的各种技术和组织措施，以确保企业的数据安全控制措施有效并得到合理实施。通过进行第三方审核和认证，企业可以向客户、合作伙伴和利益相关者展示企业对于隐私保护和数据安全的高度重视。认证的结果将被公开，以增加透明度并建立信任，并根据他们的评估结果不断完善企业的隐私保护和数据安全措施，以确保企业始终处于符合最佳实践的状态。

（七）建立投诉处理机制

为了增强用户的信任和满意度，企业可以建立完善的投诉处理机制，以便用户能够及时向企业提出投诉，并保障他们的隐私和数据安全。

企业可以提供多种渠道供用户进行投诉，包括但不限于在线客服、电子邮件和电话。无论用户选择哪种方式，都需要确保投诉信息被及时收集并进行记录。一旦接收到用户的投诉，企业要迅速采取行动，调查问题并解决纠纷。在处理投诉过程中，企业也要尊重用户的隐私权和数据安全，承诺不会未经用户同意将其个人信息泄露给第三方，并采取必要的安全措施来保护用户的隐私和数据安全。

五、结语

在数字化时代下，企业合规中的隐私保护和数据安全问题至关重要。通过遵守法律法规、加强内部管理、加强员工培训、建立政策、进行第三方审核和认证、建立投诉处理机制以及与相关机构合作，企业可以更好地保护用户隐私并确保数据安全。只有通过合规措施的落实，企业才能在数字化时代中获得可持续发展和用户信任的基础。

参考文献

[1] 黄晓晓.社交网站隐私侵权及保护研究——基于个人信息与数据安全视角[J].今传媒，2016，24(1)：51-54，61.

[2] 安柯颖.个人数据安全的法律保护模式——从数据确权的视角切入[J].法学论坛，2021，36(2)：58-65.

[3] 高轶峰，左超.企业隐私保护工作的挑战和实践探索[J].中国信息安全，2021(3)：89-91.