

数据隐私和网络安全

数据泄露和隐私问题可能导致高昂的计划外费用和业务中断，以及强制性执法行为和潜在诉讼。单是发生数据泄露就会对企业的声誉造成重大损害。此外，越来越多的网络威胁催生国内和国际数据隐私法，这些法律对不合规行为进行处罚，并在广泛的法律执业领域产生其他影响。企业如不采取充分措施（法律、运营和技术上）解决此类事宜和准备应对这些事件，往往会将自身置于危险之中。

Archer 的数据隐私和网络安全团队律师在提供数据隐私和网络安全相关服务方面采取多学科方法，利用来自事务所多个业务领域的律师经验，包括商业咨询、劳动和就业、医疗保健、诉讼、知识产权、商业法和交易以及政府事务。

与客户内部或预留的信息技术、数据安全和保险专业人员携手，我们帮助客户针对其隐私和数据安全问题制定具体解决方案，遵守法律和监管要求，形成其业务做法，以避免代价高昂和具有威胁性的法律和监管暴露并以最佳方式预防网络事件，并在客户遭受数据泄露或其他受法律保护或机密信息丢失的情况下最大限度减少暴露。

我们还管理调查过程、就法律通知和报告要求提供建议以及就个人或政府实体可能对客户提起的任何索赔或诉讼提供建议和辩护，从而帮助客户应对网络事件或数据泄露。我们了解监管机构的期望、他们如何调查和执行数据保护问题，以及最适合客户取得积极成果的策略。