Information Privacy, Security and Data Rights

Primary Contact

Anton L. Janik, Jr.
P. (501) 688.8888
E. ajanik@mwlaw.com

Attorneys

Benjamin D. Jackson
Zachary T. Steadman
Jeff McWhirt

Confidence for your foreign and domestic data privacy, compliance and risk-response needs.

Data privacy law is at the forefront of business concerns today, with increased focus on data subject rights; domestic and international regulatory and legal compliance; identifying, assessing and addressing cybersecurity threats, cyberattacks and ransomware; wide-ranging regulatory penalties and legal liabilities; and correspondingly-limited cyber insurance coverage.

Businesses, organizations and governmental entities of all sizes, across all industries, face privacy and security risk arising from the data they collect and use – which is why so many depend on the Information Privacy, Security & Data Rights team at Mitchell Williams for their data privacy, security compliance and risk-response needs.

We combine extensive experience and business knowledge to help clients comply with regulatory and legal requirements, both domestically and internationally, and mitigate risk before, during and after an incident. How? By understanding data collection, transfer and usage practices. Knowing the legal impact and regulatory weight placed on business operations. And providing legal strategies that bring data handling practices into regulatory compliance, at the lowest possible organizational burden.

HIGHLIGHTS

- Certified Information Privacy Professional (CIPP) attorneys, holding both United States and European privacy certifications
- Former U.S. Department of Justice attorney
- Deep understanding of industry-specific domestic and international laws and requirements in health care, financial, cryptocurrency, sales and marketing, insurance, retail, nonprofit, professional services, education, utility, manufacturing, transportation, government and real estate
- Early identification of issues and development of strategies to help clients become data privacy compliant, remain compliant, and mitigate or avoid penalties for noncompliance

CAPABILITIES

Data Privacy Regulatory Compliance

- Develop and evaluate comprehensive organizational and website information privacy policies and procedures for customer and employee data, including acceptable use, terms of service, terms of use, terms of sale, popup cookie disclosures, intercompany data sharing agreements, data transfers using Standard Contractual Clauses, and Data Processing Agreements
- Direct data inventory mapping exercises

- Address data collection and limitation of use concerns
- Assist with metrics for, and evaluation of, risk associated with data collection and processing
- Prepare strategies to respond to Data Subject Access Requests
- Draft and negotiate customer and third-party data access and use agreements
- Provide guidance to evaluate vendor risk and address same through Business Associate Agreements
- Draft and negotiate vendor questionnaires, vendor contracts, Business Associate and Information Security Agreements
- Assist with ongoing monitoring and evaluation of vendors
- Advise on data privacy issues related to e-commerce, mergers and acquisitions, international data transfers, outsourcing, online marketing, contests and sweepstakes, and loyalty programs

Information Security Management Practices

- Develop and evaluate comprehensive organizational and website information security policies and procedures for customer and employee data, including access control, change management, business continuity, disaster recovery, records retention, password management, remote access, bring your own device, disposal, clean desk, authentication procedures and encryption
- Review insurance policies to analyze scope and gaps in cybersecurity coverage
- Prepare responses for third-party audits and regulatory examinations and inquiries
- Analyze transactional and operational risk, including due diligence review for mergers and acquisitions
- Advise on security issues related to international data transfers and outsourcing of processing, hosting and storage
- Assist with ongoing monitoring and evaluation of vendors

Data Incident Response Program Development & Support

- Create and evaluate incident response plans
- Recommend strategic and tactical risk remediation measures to minimize risk exposure
- Assist with simulated data breach exercises and analysis of findings
- Direct internal investigations and responses to security incidents
- Assist with risk of harm evaluations related to security incidents
- Prepare materials and strategies for covered entity and consumer breach notifications
- Assist in the preparation and review of security incident remediation plans
- Collaborate with law enforcement, notification vendors, forensic investigators, insurance providers and crisis communication professionals
- Defend clients in investigations of security incidents by states attorneys general
- Defend covered entities in security incident investigations brought by the Office of Civil Rights, Department of Health and Human Services (OCR)

Laws & Requirements: International, Federal & State

- State data use and privacy statutes and regulations, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- International data use and privacy statutes and regulations, including the General Data Protection Regulation (GDPR) and Data Protection Act of 2018 (UK GDPR)
- State financial privacy regulations including the New York Department of Finance Cybersecurity Regulations
- New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Freedom of Information Act (FOIA) and similar state laws

- Federal Trade Commission Act including "Red Flag Rule"
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transactions Act (FACTA)
- Bank Secrecy Act and other Anti Money Laundering (AML) laws
- Healthcare Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Telephone Consumer Protection Act (TCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- U.S. state laws, including data security and notification laws
- Securities and Exchange Commission (SEC) cybersecurity disclosure requirements
- Video Privacy Protection Act (VPPA)