Buchanan

DATA PRIVACY AND PROTECTION

NetDiligence AUTHORIZED BreachCoach

The era of unfettered personal data collection is over. Accountability has arrived. Experienced, leading-edge counsel is key.

Consumer demands and regulatory requirements are making data collection and use more complex by the day. And, companies face enforcement and litigation if they cannot show that they used reasonable security measures to safeguard personal data. Having the most up-to-date privacy policies, procedures and compliance program has never been more important.

Buchanan Ingersoll & Rooney is a recognized leader in data privacy law and designing programs to protect privacy. We offer strategic legal counsel for clients who collect and process data from consumers, employees, job applicants, business partners, research subjects, patients, students, and website visitors.

How We Can Help You

Privacy Team

Privacy legislation, regulation, and enforcement have exploded over the past few years, placing the burden on companies to build a privacy program in a legal environment that is demanding, complex, and constantly evolving. It requires technical know-how that often exceeds the resources of many organizations.

Our dedicated privacy team is committed to helping you address the risks, priorities, and practical implementation actions best suited to your unique mix of data collection, use, sharing, protection, retention, and regulatory environment. We collaborate with our colleagues in employment law, intellectual property, healthcare, financial services, consumer protection law, and other disciplines for industry-specific insight. And, our government relations professionals help anticipate future developments at the federal and state executive, legislative and regulatory levels.

Data Security Team

Data security is essential to privacy compliance, whether by statute, rule, contract, or case law. In most states, “reasonable security measures” are mandated for many types of personal data. The technically skilled and experienced cybersecurity arm of our data protection team works with you to develop a defensible security program that meets prevailing legal and industry standards to protect data privacy and is tailored to your specific capabilities.

Data Privacy Counseling and Compliance

We work with you to identify the privacy and data protection laws and regulations that apply to the specific types of data collected. We help integrate these requirements with organizational operations and long-term planning, including compliance with:

- New and differing "comprehensive" data privacy laws enacted in multiple states
- Requirements for privacy policies, digital advertising, website consents, and preference selections
- Federal Trade Commission regulations and enforcement actions targeting consumer data protection
- State regulatory action and court rulings on data privacy and security under consumer protection laws
- Federal and state action on the privacy risks of artificial intelligence (AI)
- Sector-specific requirements for healthcare, financial services, education, and government contractors
- Federal and state "reasonable security" requirements for personal data
- Health data privacy and breach notification compliance for organizations, whether subject to HIPAA or not
- Supply chain risk management, including third-party risk management and data protection agreements, and provisions for commercial contracts
- Workforce privacy and security requirements and training

Data Mapping

Understanding where all the legally protected data in your environment is located, who has access to it, and how long it should be retained is easier said than done. Our team works with your legal and information technology (IT) teams to develop practical, prioritized data mapping programs with both privacy and cybersecurity objectives. For privacy, a full understanding of data collection, storage, and access is essential to a complete and accurate privacy compliance program. For cybersecurity, knowing where data is located is critical for IT and legal counsel to prioritize what to protect and to understand the legal consequences of potentially compromised data.

Risk Assessments

New state privacy laws mandate data protection assessments for data-related activities that pose a risk of substantial privacy harm, such as processing health, geolocation, and other sensitive data; targeted behavioral advertising; consumer profiling; and automated decision-making. Basic data protection principles require due diligence of third parties who may have access to your IT environment or confidential data, regardless of whether data usage is within the service scope. We help create the tools, conduct the gap analysis, document the assessment process, and draft the contract protections necessary to meet your compliance priorities.

ADVANCING OUR CLIENTS' GOALS

Below are some of the ways we have helped our clients' data privacy and protection programs succeed:

Strategic Counseling

- **Assisted an EU-based international e-commerce retailer entering the U.S. market to understand and comply with U.S. data protection laws.**
- **Provided strategic counsel to a publicly traded real estate company spanning multiple sectors to navigate and document compliance with new state privacy laws.**
- **Advised a leading security alarm and emergency response company operating in residential, commercial, and business services sectors on meeting data protection regulations under state laws.**
- **Conducted comprehensive reviews and negotiations for a community bank on commercial and data protection terms within master services agreements and related statements of work for IT managed services and managed security services.**
- **Guided a U.S. pharmaceutical company in understanding and complying with the General Data Protection Regulation for a clinical trial involving study sites in the European Union.**
- **Assisted a provider of support services for patients with critical medical conditions and their caregivers in establishing secure data collection and website practices that protect patients' sensitive information.**

Privacy Litigation

- **Successfully obtained a dismissal of all claims in a Florida invasion of privacy case alleging wiretapping violations on the client's website, and received a favorable ruling from the arbitrator in a CA invasion of privacy in a website wiretapping case, with the client prevailing on all counts and no award granted to the plaintiff.**
- **Secured a second consecutive dismissal for a global apparel manufacturer in a class action lawsuit involving CA invasion of privacy/CA wiretapping, closing the case in our client's favor after the plaintiff chose not to amend for a third time.**
- **Secured dismissal of wiretapping, medical information act, CCPA, and other privacy claims against our online pharmacy client in a putative class action.**

Transactional Data Protection

Data is an essential component of commercial transactions and M&A deals. We help buyers and sellers, customers and service providers to analyze and reduce data-related legal risks, including:

- Assessing data protection risks of companies involved in mergers and acquisitions
- Assessing data protection risks in commercial contracts
- Preparing customized representations, covenants, and remedies to protect against third party liability
- Negotiating data protection agreements to address specific transactional risks and comply with U.S. laws and the European Union's General Data Protection Regulation (GDPR)

Privacy & Data Protection Litigation

Courts are treating data protection with the utmost concern and are holding companies accountable for their failures. Cybersecurity breaches and data privacy violations can have severe consequences for individuals and organizations alike. If a breach does take you to the courthouse or finds you defending actions by regulatory agencies, our litigation team – highly experienced in post-breach suits – will defend you in any form of litigation in any venue, whether single-plaintiff lawsuits, class actions, mass or individual arbitrations, or actions brought by regulatory authorities. We treat privacy and data security litigation as a distinct legal field, recognizing the specialized knowledge necessary for achieving success in such cases.

Our team of litigators possesses in-depth understanding of the laws that affect privacy and data security litigation. These include the federal Electronic Communications Privacy Act, encompassing the Wiretap Act and the Stored Communications Act, the California Invasion of Privacy Act, the California Consumer Privacy Act, the Video Privacy Protection Act, the Fair Credit Reporting Act, and the Telephone Consumer Protection Act. We are well-versed in the state-level counterparts to these statutes, state consumer protection laws, and common law privacy torts.

For additional information, contact our Cybersecurity & Data Privacy leadership team or email us at cyber@bipc.com.

SUE C. FRIEDBERG
Co-Leader of Buchanan's Cybersecurity and Data Privacy Group
sue.friedberg@bipc.com
412 562 8436 | Pittsburgh, PA

MICHAEL G. MCLAUGHLIN
Co-Leader of Buchanan's Cybersecurity and Data Privacy Group
michael.mclaughlin@bipc.com
202 452 5463 | Washington, DC

JENNIFER M. OLIVER
Shareholder
jennifer.oliver@bipc.com
619 685 1990 | San Diego, CA

KURT SANGER
Cybersecurity Counsel
kurt.sanger@bipc.com
813 222 1103 | Tampa, FL

HARRY A. VALETK
Shareholder
harry.valetk@bipc.com
212 440 4416 | New York, NY

BIPC.com/cybersecurity-and-data-protection