Cybersecurity, Data Protection & Privacy

Protection of the security and privacy of information and data presents an ongoing and growing challenge to individuals, businesses, and enterprises of all sizes.

A comprehensive and interdisciplinary approach to data management is critical in today's climate, in which all operations across all private and public sector verticals are becoming digitized, each with its unique data flows and information management opportunities and challenges. On the one hand, controlling data and exploiting its value can be a key ingredient to maintenance and increase in enterprise value. On the other hand, increased dependencies on digital devices and networks have been associated with increased vulnerability of data to breach due to systems deficiencies, human error, and malicious attack. These exposures have correlated with an intensification of regulatory oversight, enforcement, and civil actions.

DATA BREACH HOTLINE: 877.912.9470

Clark Hill offers our Cybersecurity clients a "24/7" data breach hotline at 877.912.9470. In the event of a suspected breach our team will assess the data security incident, its impact on personally identifiable information, and whether it triggers breach notification obligations.

Cybersecurity, Data Protection & Privacy Leaders

Melissa K. Ventrone
+13123602506
mventrone@clarkhill.com

Jeffrey R. Wells
+12026406682
jwells@clarkhill.com

In this dynamic environment, the full array of corporate activities is increasingly being driven by the opportunities and risks associated with the collection, maintenance and dissemination of data. Compliance initiatives, mergers and acquisitions, cloud and other vendor contracts, consumer-facing e-commerce offerings, product development, software development, insurance and corporate reputation generally (just to name a few) are increasingly being driven by the opportunities and risks associated with data.

Clark Hill's team approach to data protection brings together security and privacy attorneys with colleagues from our core practice groups and sector and service teams to tailor our services to each client's unique data, privacy and security needs. Our team understands technology and the related legal issues and challenges and is accustomed to working with our clients' own technical, business, marketing, compliance and other stakeholders.

We provide practical, forward-looking solutions that empower our clients to maximize and protect the value of their data in many industries, including financial services, technology energy, food and beverage, manufacturing, retail, services, healthcare, and pharmaceuticals. The Clark Hill team is familiar with a broad array of financial technology (fintech), including blockchain, distributed ledgers, robo advice, and smart contracts, to name a few.

Our counseling, transactional, compliance and remediation work covers a range of industries and corresponding regulatory regimes, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley (GLB)
- The Federal Trade Commission Act
- Federal Fair Credit Reporting Act
- The Electronic Communications Privacy Act (ECPA)
- Industry-specific requirements for financial services, health care, utilities, transportation, education, and government contractors
- The Health Insurance Portability and Accountability Act (HIPAA)
- State consumer data protection laws
- State data breach notice laws
- Safeguarding consumer credit information
- Identity theft "red flags"
- Secure disposal
- The European General Data Protection Regulation (GDPR)
- The Child Online Privacy and Protection Act (COPPA)
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM-Act)

Areas of Cybersecurity, Data Protection & Privacy Legal Services

Security Incidents: Preparation, Response and Remediation

- Response planning
- Analyze and evaluate cyber insurance coverage options
- Breach investigations
- Incident response
- Preparation of notice to affected individuals
- Dealing with law enforcement, insurers, public relations, and stakeholders
- Addressing claim and litigation issues (including class action defense, “cyber torts,” and fraud)

Technology Planning and Policies

- Inventories of systems, devices and data
- Risk assessments
- Consumer facing privacy and security policies
- Internal policies, including privacy and security policies, technology acceptable use policies, communications policies, BYOD (bring your own device) policies, retention and destruction policies, crisis management and breach policies, and facilities management policies.
- Training
- Compliance audits
- Cross-border data transfer
- Outsourcing, development, and licensing
- Governance, risk, and compliance

Business and Consumer Transactions

- Optimizing ownership, rights and monetization of data
- Securing data rights in licenses and other transactions
- Due diligence on data management/compliance in M&A and other key transactions
- Negotiating risk allocation, warranties and other key provisions relative to data protection and disaster recovery in cloud services, software as service, hosting and other contracts.
- Negotiating contracts for security products and services
- Counseling on cross border data transfer and other international risks
- Drafting consumer facing privacy policies, terms of use and end user license agreements for websites and mobile apps
- Negotiating website and app development agreements with reference to data protection design components and obligations

Our Cybersecurity, Data Protection & Privacy attorneys work closely with the professionals in Clark Hill's Information Governance and Discovery Services to provide multidisciplinary solutions for our clients.