Whether managing sensitive employee and customer data or connecting to the ever-growing Internet of Things, the information that companies collect, create, and manage is a valuable business asset of ever-increasing importance. In addition to cultivating the benefits that information and data provides, companies need to understand how to manage, and discern the risks that arise out of, the gathering, maintenance, dissemination, and disposal of information. To effectively address these challenges, companies must take proactive measures to protect these sensitive assets, comply with rapidly evolving legal requirements, and still enable optimal business performance.

Honigman’s Data, Privacy and Cybersecurity group helps clients develop effective solutions that protect and manage information assets, comply with complex and rapidly changing areas of law, respond to data breach and other security incidents, and address claims of privacy violations. Our group is a multidisciplinary team of attorneys and professionals who assist clients to holistically manage the lifecycle of data, including addressing issues involving data use, licensing, privacy and security -- to promote innovation, protect corporate information, and reduce risk. Our team has extensive experience and skill as litigators, technology transaction professionals, and regulatory and investigative lawyers managing data in all industries, including automotive, tech, manufacturing, retail, hospitality, health, education, and financial services. We help manage risk without impeding business growth. We advise clients on how to develop comprehensive programs designed to identify and address potential threats, collect and use information that adheres to compliance and regulatory frameworks, and protect information assets. Several of our attorneys and staff are Certified Information Privacy Professionals, a certification from the International Association of Privacy Professionals, the world’s largest and most comprehensive global information privacy organizations.

How We Help

We assist clients to harness the power of their data while helping clients minimize information risks, and, when necessary, respond to data privacy or security compliance and remedial matters. Our core areas of capability include:

**Data licensing and commercial agreements.** Our team assists companies to prepare agreements to optimize and monetize data assets. For example, we help clients with the following:

- Advising clients in B2B and B2C data licensing and sharing transactions
- Representing clients in negotiation of SaaS, PaaS, NaaS and IaaS agreements and implementation
- Counseling clients concerning the management of “big data” through artificial intelligence and machine learning
- Negotiate, draft and advise clients on a broad range of commercial contracts in which data and personal information are key assets or issues

**Cybersecurity and privacy programs.** Effective information management requires a careful balance of proper use, protection and risk reduction policies and procedures. We help clients ensure that information use adheres to necessary legal and regulatory requirements without unduly burdening the business. We regularly
offer guidance in the following:

- Developing strategies for information collection, use, storage, and disposal
- Creating internal programs and processes for managing information, such as privacy impact assessments, vendor due diligence, privacy by design, and internal training
- Drafting necessary privacy policies, including website privacy notices, terms and conditions, written information security policies (WISP), and incident response plans
- Assessing privacy risks and developing associated mitigation plans
- Evaluating cybersecurity programs and remediating gaps

**Regulatory compliance.** Numerous cybersecurity and privacy regulatory and legal frameworks govern the collection, use, disclosure, storage, and destruction of information, both domestically and internationally. Navigating these often-complex regimes can prove challenging. We routinely advise clients on how to best manage their compliance efforts, including the following:

- Advising on various privacy obligations under domestic and international regulations such as the California Consumer Privacy Act (CCPA), HIPAA, Gramm-Leach-Bliley Act (GLBA), the EU General Data Protection Regulation (GDPR), the Family Educational Records Privacy and Act (FERPA) and the Illinois Biometric Information Privacy Act (BIPA)
- Understanding the priorities of domestic and international regulators and responding to enforcement actions emanating from the U.S. Federal Trade Commission, European Data Protection Authorities, and other regulatory bodies
- Developing adequate cross-border data transfer mechanisms, including self-certifying with EU-U.S. Privacy Shield, the implementation of the European Commission’s standard contractual clauses, and/or binding corporate rules
- Representing clients in investigations involving privacy or data security brought by the FTC or state attorneys general

**Cyber insurance.** The proliferation of threats to corporate information and technology systems necessitates adequate protection, including insurance coverage. Our experienced policyholder attorneys represent clients on a wide array of cyber-insurance matters, including the following:

- Advising clients on coverage issues in the event of a data breach or related loss
- Maximizing coverage and reimbursement from the insurer in the event of a loss
- Representing insureds in coverage litigation when it becomes necessary or inevitable
- Counseling insureds on understanding the coverage they are purchasing
- Understanding how best to protect their companies before, during, and after a security or privacy incident

**eDiscovery and information management.** Most privacy principles stress the importance of retaining information only as long as necessary, and effective information and records management practices ensure
companies meet these requirements. Our attorneys routinely assist companies in integrating information management practices into privacy programs and practices, including the following:

- Developing records retention schedules and records management policies
- Advising on the records retention and privacy implications of changes in technology use
- Assisting in the development of comprehensive records destruction practices

**Incident response.** Many companies will experience some type of data security incident or loss, and managing the response to such an event is often complex and burdensome. We have extensive experience helping clients prepare for and respond to data breach and security incidents, including the following:

- Identifying and remediating possible data security and data breach risks
- Developing a data breach response plan
- Assisting with selecting vendor and consultants
- Investigating the scope and cause of data breaches
- Coordinating data breach response efforts
- Executing a multi-jurisdictional notification strategy

**Privacy and data security litigation.** Should litigation occur, we aggressively defend our clients, including in class actions on both the state and federal level related to negligence, privacy statutes, credit monitoring claims, state breach response laws, and more. Our team includes former plaintiff class action attorneys, government prosecutors, and skilled civil litigators who defend clients in a wide-range of litigation involving privacy and data security matters, including:

- Biometric laws, including the Illinois Biometric Information Privacy Act (BIPA)
- State data breach notification laws
- Various state privacy laws, including the Michigan Video Rental Privacy Act
- Federal privacy laws, including the Fair Credit Reporting Act (FCRA), the Telephone Consumer Protection Act (TCPA), and the Wiretap Act
- Federal government investigations and litigation, including involving the Federal Trade Commission and state attorneys general