Cybersecurity Counseling and Compliance

It’s not a question of if a cybersecurity incident will occur. It’s a question of how prepared you will be when it does.

About

Cybersecurity incidents are no longer extraordinary events. Organizations of every size, from the largest global brands to emerging companies, need to plan for the unauthorized disclosure of personal information. When a cybersecurity incident occurs, the consequences are immediate: government investigations, regulatory enforcement, consumer litigation, and lasting reputational harm.

Understanding the Risks

The regulatory landscape is intensifying. Federal and state regulators, industry standard-setters, and consumers all demand more rigorous data protection, and the legal obligations governing how organizations prepare for and respond to security incidents grow more complex each year. In this environment, experienced cybersecurity counsel is invaluable. The right counsel helps organizations build resilient incident response plans, craft defensible data-governance policies, navigate evolving disclosure and notification requirements, and engage with regulators from a position of preparation. When an incident does occur, that groundwork can be the difference between a manageable response and a crisis.

Our Cybersecurity Counseling and Compliance team works with companies to manage cyber risks and, where necessary, effectively resolve data breaches in compliance with state, federal, and industry regulations. We serve clients in highly scrutinized industries, including health and financial services, consumer products and retail, hotel and leisure, telecommunications, and technology services.

Regulatory Guidance

We counsel clients on privacy and data security matters, helping them navigate the complex landscape of laws, regulations, and guidance that govern the collection, use, and protection of personal information. Our team advises on managing risk and reducing liability related to both consumer and employee data, and we help clients develop and implement compliant business practices that meet applicable industry self-regulatory requirements.

Our counseling spans the full range of privacy and information security requirements, including:

- U.S. federal and state privacy and data security laws, such as the Federal Trade Commission Act, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Children’s Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), and the CAN-SPAM Act;
- Sector-specific obligations, including the Communications Act, Customer Proprietary Network Information (CPNI) regulations, and the Payment Card Industry Data Security Standard (PCI

DSS); and

- International data protection regimes, including the EU General Data Protection Regulation (GDPR) and other national and local privacy laws worldwide.

Compliance Programs and Training

Our attorneys help clients draft, review, revise, and interpret their privacy, data security, and CPNI policies and procedures, and develop comprehensive, enterprise-wide privacy and data security programs designed to withstand regulatory scrutiny and reduce exposure in the event of audits, investigations, or enforcement actions. We conduct employee training on data security practices and perform data security assessments regarding compliance with applicable laws, regulations, and internal policies. We also assist clients in developing and implementing oversight and monitoring policies for third-party vendors that handle consumer data, promoting clarity around responsibilities and risk allocation, strengthening compliance, and mitigating exposure if a vendor mishandles personal data.

Incident Response

We help clients proactively develop policies and procedures to avoid data breaches and meet their legal obligations when a cyberattack or other cybersecurity incident occurs. We regularly advise companies facing regulator-led investigations and multistate enforcement actions following cybersecurity incidents. We advise on internal and third-party forensic investigations to determine the source and scale of the data incident, assist in meeting consumer and regulatory notification obligations, manage public relations, and counsel on overall strategy to reduce the risk of resulting investigations and litigation.

Related Services

General Data Protection Regulation (GDPR)
Technology
Federal Trade Commission
Privacy and Information Security

Contacts

Alysa Z. Hutnik
ahutnik@kelleydrye.com