# Cybersecurity, Data Protection & Privacy

## OVERVIEW

Attorneys in Eckert Seamans' Cybersecurity, Data Protection & Privacy practice group have a deep understanding of data security and privacy requirements across a variety of industries and sectors, including laws pertaining to consumer products, retail, health care, labor and employment and telecommunications. Our experience allows us to provide our clients with practical, cost-effective, and results-oriented counseling regarding the protection of personal and other sensitive information.

Through the rapid evolution of technology, threats to data security are multiplying. Laws and regulations are changing and expanding, imposing complex and often inconsistent privacy and data protection standards. At the same time, the legal and business risks associated with non-compliance with emerging regulatory requirements have escalated. For these reasons, we invest significant time and resources in counseling clients on laws relating to the collection, use and protection of personal information as well as on mitigating risks and reducing exposure to investigations and litigation arising from the loss, theft or exposure of personal data.

Our clients trust us to guide them through all stages of breach matters, including prevention and compliance, response and notification, government investigations and regulatory response, and, when necessary, litigation.

## BREACH PREVENTION AND COMPLIANCE

Data incidents are a reality for organizations large and small. Working with trusted advisors to develop and implement a data breach prevention strategy is a crucial factor in protecting assets in today's business world. Attorneys in Eckert Seamans' Cybersecurity, Data Protection & Privacy group work with clients to implement preventive measures into their daily operations. Our team also conducts privacy or data security audits of existing business practices and assists clients with privacy compliance solutions so they can operate confidently in evolving and complex regulatory environments.

The firm's Cybersecurity, Data Protection & Privacy team also assists clients with day-to-day business needs relating to data privacy and security, including training employees on privacy and data security practices that comply with consumer protection laws, developing oversight of third-party vendors that handle consumer data, and drafting/negotiation of data privacy contract terms and conditions as well as privacy policies.

## INCIDENT RESPONSE AND NOTIFICATION

In the event of a security incident, we coordinate the incident response plan and guide clients through the process of conducting internal and third party investigations to collect, preserve, and document evidence in an effort to determine the nature and source of the incident and whether it is a reportable breach under applicable law. We also advise and assist clients with notification obligations, how to deal with the reputational impact of the breach, and reducing the risk of resulting government investigations and/or litigation.

## GOVERNMENT INVESTIGATIONS AND REGULATORY RESPONSE

As part of the breach response, our team represents clients in state attorney general or Federal Trade Commission investigations and enforcement actions. We also defend clients in federal and state courts and before regulatory agencies regarding their data security and privacy policies and procedures.

## PRIVACY REGULATION AND COMPLIANCE

The Cybersecurity, Data Protection & Privacy team has developed a thorough understanding of U.S. and European laws regulating the collection and use of personal information, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). We advise clients concerning their legal data privacy compliance obligations, provide them with contract language for data

processing agreements, privacy disclosure statements for websites, and assist them with responding to data subject rights requests.

## LITIGATION

In the event that a client's government or industry-based investigation escalates to litigation or faces a class action, Eckert Seamans' Cybersecurity, Data Protection & Privacy team is adept at developing focused and cost-effective defense strategies.

## INDUSTRY FOCUSES

**Consumer Payments and Retail**
Attorneys in Eckert Seamans' Cybersecurity, Data Protection & Privacy group follows the latest trends in payment card industry (PCI) compliance requirements, including revisions in data security standards. Where a breach involves credit card data, we assist clients in dealing with payment card industry fraud cost recovery actions, fines and assessments. Retailers are subject to various state and federal laws regarding the collection, use and disclosure of customer information. We help companies minimize their risk exposure while meeting their legal and contractual obligations.

**Health Care (HIPAA and HITECH)**
We regularly advise clients on issues related to the privacy and security of health information under the Health Insurance Portability and Accountability Act (HIPAA), including compliance with the requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Our attorneys routinely design and implement compliance plans and performs audits for covered entities and business associates. In addition, our team can provide workforce training, perform breach assessment and counsel on risk assessment and documentation.

**Human Resources and Workplace Privacy Compliance**
We assist with workplace privacy compliance issues concerning the processing and safeguarding of employee personal data, employee monitoring, the implementation of whistle-blowing hotlines, responding to data access requests and conducting background checks. We also provide training to HR management on their obligations when dealing with employee data and practical steps for avoiding security breaches.

**Telecommunications Services**
We regularly advise clients on privacy issues unique to telecommunications services, including text messaging and email. The team assists telecommunications carriers and broadband service providers in establishing and maintaining policies for the protection of Customer Proprietary Network Information (CPNI), in accordance with the Communications Act and Federal Communications Commission (FCC) rules. In addition, the team counsels educational institutions, pharmaceutical companies, commercial businesses and web-based service providers on a broad range of compliance issues arising under the Telephone Consumer Protection Act (TCPA), the CAN-SPAM Act and the Federal Trade Commission (FTC) Telemarketing Sales Rule.

**Leisure & Hospitality**
Eckert Seamans serves as national data breach response counsel to one of the largest independent hotel management companies in the United States. It can be a challenge for hotels to protect the privacy and security of consumer information. Eckert Seamans understands the unique characteristics of our clients' leisure and hospitality business, which allows us to provide reliable advice concerning best practices for consumer and employee data privacy & security in these environments. We prepare data privacy policies and data security incident response plans so that our hospitality clients can minimize their risk and be prepared in advance of a breach. We also advise clients on their response and notification obligations in the event of a breach or investigation. Eckert Seamans has handled responses to dozens of data breach incidents within the hospitality industry.

**Education**
We understand the laws governing the collection and safeguarding of information concerning students gathered within the context of their educational environments, and we assist our clients in complying with those laws. Eckert Seamans has assisted public school districts and universities in responding to data security incidents.

**Insurance**
The lawyers at Eckert Seamans are familiar with insurance providers and how they operate. As a result, we

are able to provide quality counseling to the insurance industry in data privacy and security matters, including the creation of appropriate policies, planning and preparation for data security incidents, and data breach response.

**Financial Services**
Banking and financial services have been frequent and at times high-profile targets for data thieves. Eckert Seamans has knowledge of the laws and regulations that control privacy and security of consumer information within the industry. We have assisted banks in preparing data breach response plans and advised them regarding the sufficiency of their cyber insurance coverage.

## REPRESENTATIVE MATTERS

- Represented multiple hotel owners in responding to a major breach of the electronic security and theft of credit card data from a major hotel brand in an attack perpetrated by hackers;
- Handled all aspects of responding to dozens of data breaches involving both electronically stored information and paper information for large independent hotel management company;
- Assisted clinical laboratory company in responding to theft of employee personal information by hacking that resulted in the filing of numerous fraudulent federal tax returns and an attempt to compromise the company's bank account;
- Assisted a university in working with law enforcement investigators and complying with notification laws when a hacker attacked the university's online applications database;
- Provided guidance and assistance to a national online retailer when credit card data maintained within its system was accessed by an unauthorized person;
- Represented insurance provider in meeting its obligations when personal information of insurance agents was inadvertently made accessible through the insurer's web portal;
- Represented manufacturing company in working with law enforcement agencies and addressing notification duties after a rogue employee stole personal information from employee files to be used to forge prescriptions for controlled substances;
- Assisted public school district in responding to inadvertent disclosure of personal information captured in computerized database for visitor registration;
- Drafted data breach response plans and reviewed/advised on cyber insurance coverage for bank and a nonprofit legal aid organization; and
- Formulating data breach response plan, reviewing internal privacy and security policies and cyber insurance coverage for multi-state accounting firm.