

Cybersecurity, Data Protection & Privacy

Protection of customer, employee and business data is a fundamental business priority: Customers, industry standards, laws, regulations and good business practice demand that today's companies guard data like never before. And even with state-of-the-art protections and protocols in place, human error, evolving technology and creative hacking leave secure systems vulnerable to attack.

Our cybersecurity, data protection and privacy lawyers regularly represent commercial enterprises across numerous industries in a broad spectrum of cybersecurity matters, including regulatory compliance, data security policies and procedures, insurance and other contract counseling, data breach investigation and response, and data breach notification compliance and litigation. We also counsel clients on both foreign and domestic data privacy issues, including policies and procedures, regulatory compliance, enforcement and litigation. Our clients include technology companies, financial institutions, healthcare entities, investment managers, retailers and manufacturers, and e-commerce companies.

Significantly, we stay abreast of emerging regulatory developments from coast to coast: Members of our team are credentialed as Certified Information Privacy Professionals for United States (CIPP/US) and European law (CIPP/E). Our California lawyers are well versed in the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). We also advise on cross-border issues and the EU General Data Protection Regulation (GDPR).

Our Services

Security Policies and Counseling

Thoughtful data protection programs are paramount to maintaining reputation and competitive advantage. Our cybersecurity professionals assist with the assessment, development and implementation of policies and procedures with respect to data security, including customer and employee information, data retention and destruction programs, and information technology best practices. We also work with clients to strengthen, supplement and implement all policies and procedures involving:

- Access to data.
- Data destruction.
- Data retention.
- Generative artificial intelligence (AI).
- Managing Health Insurance Portability and Accountability Act (HIPAA)-protected information.
- Adherence with specific federal and state laws, including Regulation S-P and the CCPA.
- Partners and vendors that may have access to, or store, sensitive data.
- Security audits.
- Security vulnerabilities.

- Transfer of data.

We also provide comprehensive pre-breach counseling. Our lawyers are well-versed in the state and federal laws governing the protection of confidential, personally identifiable information, personal health information and other private records — and what steps are required in the event of unauthorized access. We use this knowledge to help clients assess, prioritize and address their current risks, create and implement best-in-market policies and procedures, develop incident response plans, create training programs and conduct training, and assess cyber insurance policies.

Regulation and Compliance

Our team provides advice to clients regarding privacy and data protection laws, compliance with those laws, and risk mitigation practices across numerous industries, including insurance, finance, healthcare, education, retail and consumer data. In addition, we counsel clients on the implication of compliance obligations in transactions, such as corporate governance, risk management and corporate transactions.

We work to protect clients before and after a data breach, from preparing privacy and security policies to swift guidance on responding to a data breach and issuing requisite breach notifications. Once a cyber incident investigation is underway, where a breach triggers regulatory disclosures and possible fines or penalties, our lawyers team up with our government affairs professionals to interface with state and federal law enforcement and other regulators, as well as any counterparties to whom a disclosure obligation is owed, in order to ensure legal compliance and minimize damages.

Data Breach Response

Our dedicated data breach response team understands the importance of a prompt and proper data breach investigation and response. Along with our technology partners, we help our clients take the quick and prudent actions necessary immediately following a data breach or incident to understand the scope of the compromise; evaluate the parameters and elements of unauthorized access, movement or exfiltration of data; and assess the actions needed to maintain legal compliance and mitigate damages.

We recognize there is no standard approach for a data breach response because there is no standard data breach. IT systems vary from business to business, the geneses of breaches vary widely (from criminal hacking or data theft to equipment failure or human error), and legal requirements arising from a data compromise vary from state to state, industry to industry, and breach to breach, often depending on the types of information compromised.

Vendor Management and Commercial Contracts

With the rapid development of privacy and data security laws, there is a sharpened focus on vendor compliance and commercial contract management. Sophisticated businesses recognize that their data security is only as good as their vendors' data security. These companies are increasingly implementing strict contractual terms surrounding data security and privacy through the use of integrated and independent data processing agreements (DPAs). Our team has a wealth of experience in negotiating agreements and DPAs to protect our clients where compliance is critical, on both the vendor and purchaser sides of transactions.

Litigation

Our litigators have handled a wide range of litigation in this area. We have successfully defended clients against claims rooted in data security and/or data privacy issues in both individual and class action matters. We have also counseled clients from the plaintiff side in connection with commercial disputes triggered by cyberattacks.

Our team also manages business risk before litigation and, when the time comes, effectively preserve, collect, analyze and produce data, including providing advice regarding best practices for managing data sources, forming an information governance policy and navigating all phases of the e-discovery process in a manner that achieves the best possible and most efficient results.

Cyber Insurance

Our cyber insurance lawyers regularly assist with evaluating and selecting coverage and navigating the ins and outs of existing

coverage to ensure it will provide the requisite protection in the event of a data loss. We work side by side with all manner of clients to proactively safeguard data before an incident occurs and provide counsel after a data breach regarding existing insurance coverage, as well as any statutory notification requirements.

In addition, to protect our clients against the devastating consequences of an important data loss, we assist in structuring insurance coverage as part of a comprehensive risk-management package. We review and compare insurance programs and advise on risk management issues, premium financing, and broker and agent matters.

Representative Matters

- Represented a national alumni association of a Division I university to assess and respond to a data breach incident, including investigation of the breach and notification to state regulators and affected individuals.
- Represented a multistate oncology group to assess and respond to multiple data breach incidents and prepare HIPAA-mandated breach notifications.
- Represented a religious institution in the monitoring of a breach response and undertaking of negotiation/resolution of fines and penalties imposed by the U.S. Office of Civil Rights in connection with the privacy breach.
- Represented a regional healthcare system in the reporting and monitoring of a data incident response.
- Represented a health system in responding to a U.S. Office of Civil Rights investigation in connection with an alleged HIPAA violation.
- Defended a health system in a purported class action involving alleged sharing of patient information with unauthorized third parties.
- Represented a health plan in responding to large-scale vendor breaches and advised the health plan on the vendors' regulatory and contractual obligations to report the breach.
- Assisted a financial services organization with evaluation of cyber risk and appropriate policy coverages.
- Defended financial services, retail and e-commerce entities in connection with alleged violations of state privacy and wiretapping laws.