

OUR PRACTICE

Data Protection, Privacy and Cybersecurity

Baker Donelson's Data Protection, Privacy and Cybersecurity Team offers clients access to more than 30 attorneys with experience in all areas of information management, from privacy and data security planning and design, to compliance, data breach and litigation management. We provide the resources and concise, knowledgeable counsel our clients expect to address the entire information life cycle from start to finish. Baker Donelson has been recognized as an authorized NetDiligence Breach Coach® signifying it as a top tier law firm for Data Security, Privacy and Incident Response.

We assist clients across a multitude of industries in conducting assessments of their current data privacy obligations, we institute cutting edge policies and procedures, and we train internal teams and conduct security and risk assessments.

We support our clients through all phases of a data breach and incident response, and regularly communicate with federal and state government regulators and law enforcement agencies on behalf of our clients.

Our team is vigilant about monitoring the constant flood of new privacy regulations and global legal requirements and determining how to work with our clients to develop a plan and method surrounding these new regulations. Through this unique lens, we can guide clients through every phase of the compliance process, from compliance program creation and gap analysis, to ongoing assistance with documentation and decision-making, according to each client's specific priorities and resources.

More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP), as well as other credentialing organizations. Our credentials include:

- Artificial Intelligence Governance Professional (AIGP)
- United States-focused Certified Information Privacy Professional (CIPP/US)
- Europe-focused Certified Information Privacy Professional (CIPP/E)
- Canadian-focused Certified Information Privacy Professional (CIPP/C)
- Privacy management-focused Certified Information Privacy Manager (CIPM)
- GIAC Law of Data Security & Investigations (GLEG)
- Privacy Law Specialist (PLS)
- Payment Card Industry Professional (PCIP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Qualified Technology Expert (QTE)
- Certified Information Privacy Technologist (CIPT)

Key Industries

- Health Care
- Financial Services
- Manufacturing
- Automotive including EV and Infrastructure
- Transportation

- Government Contracting
- Education

We provide thoughtful, comprehensive and dependable guidance across the following areas of service:

Privacy. Laws and regulations governing how information can be used get more complex every day. Our lawyers counsel clients on privacy issues and compliance programs for California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), Fair Credit Reporting Act (FCRA), Fair and Accurate Credit Transactions Act of 2003, Massachusetts Data Breach Notification Act, New York Cybersecurity Regulation, behavioral advertising and a myriad of other regulatory schemes such as Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB).

Information security. We advise clients on managing risk by developing and implementing policies, procedures, standards, baselines and guidelines to manage privacy, security and compliance issues. We collaborate with clients to design and implement risk management plans and programs, including security incident response plans, information privacy and security compliance plans, and business continuity and disaster recovery plans. Information security is a significant component of a company's Environmental, Social, and Governance framework, specifically how data security pertains to a company's support of social issues and human rights. We counsel clients on privacy, data security, and its relation to [ESG issues](#).

Supply chain and vendor management. The security of your vendors is just as important as the security at your organization. Whether it's the flow of information or the flow of goods and services, we help our clients implement systems to protect their information and their vendors'.

Data incident and breach response. When incidents arise, we provide real-time legal and technical advice 24/7/365. We advise on conducting internal investigations as well as communication with affected parties, regulators and law enforcement. We also advise on incident preparedness strategies.

Insurance. Increasingly, companies are turning to insurance products and services as part of managing risk and losses associated with data and/or security breaches. We advise both insurers and insureds on the legal issues associated with insurance products related to privacy, data security and cybersecurity.

Transactions. Whether collaborating with a vendor or pursuing a merger, acquisition or joint venture, it is essential that businesses address data security, privacy, cybersecurity and related compliance issues early and adequately. We advise clients on a full array of transactional issues, including contract review and preparation, due diligence, gap analyses, integration and interoperability issues, negotiation of appropriate representations and warranties, and transferability of information under international, federal and state laws and regulations.

Regulatory investigation and litigation. We advise clients in responding to federal and state investigations and preparing for litigation arising from claims associated with privacy violations, data breaches and related technology failures.

eDiscovery. Members of our team advise clients on creating and implementing document retention and destruction programs, including processes consistent with eDiscovery rules.



Representative Matters

- Assisted a consulting client with compliance with U.S. privacy laws.
- Assisted multiple clients with website terms of use and privacy notices.

- Represented a technology company in dealings with the Federal Trade Commission arising out of a computer hacking incident leading to possible dissemination of personal information.
- Provided compliance advice on the Health Insurance Portability and Accountability Act (HIPAA).
- Successfully defended hundreds of financial institutions, health systems, educational institutions, and other businesses in data security breaches and the corresponding federal and state law requirements and investigations; served as regulatory counsel in numerous privacy lawsuits.
- Co-authored thousands of pages of data security policies and procedures, presented lectures at statewide hospital training conferences and conducted daily help-line services for a hospital association's HIPAA Privacy and Security Compliance Program.
- Represented multiple data exchange companies in a variety of industries, including telecom and utilities, in a broad range of issues related to permissible use of data and collection practices.
- Assisted multiple clients with preparation of comprehensive privacy and security programs.