

大成 DENTONS

Privacy & Cybersecurity Practice

Dentons **Privacy and Cybersecurity** group operates at the cutting edge of technology and the law, working with clients to identify, quantify, mitigate and eliminate risk. Under the protective umbrella of attorney-client privilege, a team of experienced attorneys, in coordination with elite intelligence, military and cybersecurity leaders, works to ensure that our clients can protect their information and assets around the world, including enhancing their data practices, and their ability to identify and mitigate both internal and external cyber threats and the ever-changing regulatory compliance landscape, all while effectively responding to security crises.

Our Privacy and Cybersecurity group works with clients to achieve their business goals, deploy new and innovative technologies, implement intelligent data strategies, and mitigate data-related risks. Many members of the team are individually recognized as leading lawyers in their markets. Leveraging the experience of our global team, Dentons offers comprehensive advice globally that helps our clients navigate the rapidly evolving privacy and cybersecurity landscape with a focus on expanding market share and deepening customer trust rather than merely regulatory compliance.

Our collaborative approach to partnering with our colleagues across the globe allows Dentons to provide efficient service both substantively and from a responsiveness standpoint, while providing uninterrupted, relevant services to your legal and business teams.

We understand that clients plan to position themselves in the marketplace as an innovative organization and use their unique data as a core asset. Dentons' differentiator is our ability to assist you with the proper level of practical advice, both domestically and globally, in a coordinated fashion.

As you know, the collection, use and storage of personal information is subject to an increasingly complex framework of laws and regulations both domestically (CCPA) and abroad (GDPR). Monetary penalties for violating these laws are severe and reputational damage

can be irreparable. Penal sanctions also exist, which highlights the importance afforded to protection of personal information.

Dentons leverages our knowledge of these requirements to design real-world strategies to provide bespoke advice designed to take existing compliance programs and adapt them to meet new regulatory requirements. We work with you to strengthen and implement an integrated risk management program that creates an ideal environment for innovation. As part of our commitment to provide our clients with the highest quality of service, our team provides integrated solutions rather than fragmented, impractical compliance advice that is so common in the marketplace.

Our global footprint and excellent relationships with regulators enable us to provide you with integrated and comprehensive advice. We are known for providing pragmatic and business-friendly advice with a focus on identifying and implementing best practices, as well as documenting them in a manner that facilitates and documents compliance.

KEY SERVICE AREAS

Enterprise risk assessment. We can develop a business-led, information asset-centric, enterprise-wide privacy and cybersecurity analysis of your organization's risk that provides insight to your enterprise risk management (ERM) capability. We can also provide annual updates to ensure that your organization's ERM program aligns with your changing operations, needs and priorities.

Privacy and security program evaluation. We can evaluate your organization's existing security program for compliance with existing regulatory frameworks. This is often most useful before a compliance event or audit and helps to drive the next phase of growth for your security and ERM programs.

Targeted cyber and organizational resilience good hygiene review. We have designed a review that is less exhaustive than what is required by NIST or ISO standards but which targets areas where you can immediately "buy down risk." Areas where we believe a review of critical policies and related process would significantly reduce your threat risk, include (1) hardware and software asset management, (2) risk assessments, (3) administrative privileges, (4) vendor management, (5) maintenance and auditing, (6) malware defenses, (7) data mapping/protection/recovery, (8) training and (9) incident response. We would also propose remediation measures wherever we find policies or processes wanting. A mapping of answers to your current or future control standard frameworks will also be included to ensure that what we propose is compatible with your ongoing compliance activities.

Vendor risk management. We can assess the risk that a prospective vendor may pose for your organization. Our risk-assessment framework incorporates all legislative, regulatory and industry requirements. In addition to helping you make informed decision about which vendors to hire, our framework also includes guidance on when to reassess a vendor to ensure that your supply chain partners are doing what's expected of them to prevent unauthorized access and to fully secure your assets.

Insider risk assessment. We can conduct a detailed evaluation of existing internal security and personnel policies, employee vetting procedures, physical security and electronic information security access control by job function and role, contractors vs. employees, cyber technology solutions, legal and regulatory considerations, internal resource constraints, and any recent corporate incidents.

Physical security. The nature and target of attacks on corporate entities is rapidly evolving, and not in a good way. While regulatory hurdles and cyber threats loom large, physical security is every bit as important as IT security. No matter how logically secure your organization's systems are, you have to keep unauthorized personnel from entering the place where these systems are located. We can help implement the necessary policies, procedures, and on-site tools, be they cameras, armed guards, locks, etc., to prevent access to your premises' sensitive areas.

Training, table-top exercises and executive briefing. We can develop a privacy and cybersecurity training program, customized to your operations and relevant your employees, and deliver it to your employees on-site. This includes table-top exercises that simulates cybersecurity incidents to train your incident response staff and test your incident response plan. We would also issue a report and explain our findings and recommend corrective actions to your executives.

Incident response. Our lawyers and professionals have experience advising companies on a wide range of data breach response issues, including compliance with data breach reporting requirements, coordinating with law enforcement and communicating with regulators, including the US Federal Trade Commission (FTC) and state attorneys general in the US. We have complete capabilities to help you prepare for, monitor and counter cyber and privacy threats, and to prosecute bad actors to put the financial responsibility where it belongs.

Business intelligence and due diligence. We offer various levels of advisory services, each specifically tailored to meet a client's precise needs, from producing detailed reports on particular countries to conducting complex due diligence on potential partners.



Access control and vulnerability assessments.

We help clients establish protocols for granting necessary permission and establishing authentication, including identifying and monitoring rogue access points. We advise on vulnerabilities that may exist outside your network, from known cyber criminals (including state actors, ideological groups and organized crime). And we assist with third-party risk management, from establishing a due diligence process for critical outsourcing and subcontracting arrangements to ensuring that vendor contracts include detailed cybersecurity obligations.

Security intelligence. Trust Dentons to assist you in obtaining actionable threat intelligence, internal and external, in a timely manner. This includes providing “situational awareness” of the latest malware threats, recent targets, new groups organizing attacks and links among companies, organizations, locations and technologies. Forewarned is forearmed: Threats made public ahead of time or key dates to watch that could be touch points for attacks driven by sociopolitical agendas are also on our radar.

Corporate governance. Regulators, shareholders and other stakeholders expect that data security will receive oversight from corporate boards and executives. Corporate governance of data security also requires a continuous process for risk assessment, re-assessment and management. We specialize in advising clients with their thorniest corporate governance issues, and we can help you adapt leading cybersecurity corporate governance practices to your company’s unique structure and culture.

Legal gap analysis. We apply our legal capabilities and rigorous understanding of current law and new legislation, court decisions and best practices to assess how international and local laws and regulations may apply to your current data security and privacy practices. Dentons’ lawyers have a sophisticated knowledge of applicable rules, including FTC enforcement policies, the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard, the Electronic Privacy Protection Act, California’s Confidentiality of Medical Information Act and Online Privacy Protection Act and cross-border privacy rules from the EU to the Asia-Pacific region.

MOST IMPORTANT SERVICE OF ALL

We believe that only by having a holistic and integrated privacy and cybersecurity program can an organization attain true organizational resilience. That is why, whatever the scope of work we are engaged to perform, we make sure that it is not viewed in isolation. Every privacy and cybersecurity function must be considered in the context of parallel or related activities and be managed by a cross-functional team.

Contacts



Todd D. Daubert

Partner, Washington, DC
D +1 202 408 6458

todd.daubert@dentons.com



Callie L. Pioli

Managing Associate, New York
D +1 212 398 5298

callie.pioli@dentons.com



Peter Stockburger

Senior Managing Associate, San Diego
D +1 619 595 8018

peter.stockburger@dentons.com



William M. Krouse

Associate, Washington, DC
D +1 202 496 7076

william.krouse@dentons.com

ABOUT DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

[dentons.com](https://www.dentons.com)

© 2019 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see [dentons.com](https://www.dentons.com) for Legal Notices.