Privacy & Data Security

Our Privacy & Data Security Team is designed to effectively and efficiently serve companies of all sizes, from startups to Fortune 500, and across industry sectors at every stage of the data lifecycle. Data regulation is dictated by complicated and intersecting privacy and data protection standards. Our dedicated team offers experienced guidance in multinational, federal and state privacy regimes, including GDPR and CCPA.

Our experienced and technologically savvy attorneys provide full service representation to companies building or utilizing emerging technologies such as robotics, drones, AI, Internet of Things devices, biometrics and blockchain, from DevOps to employee tracking to market entry and beyond. Clients operating in highly regulated industries benefit from our slate of attorneys with decades of experience to resolve industry-specific privacy concerns, including HIPAA considerations, consumer financial data implicating Graham-Leach Bliley applicability, and marketing practices under CAN-SPAM and the TCPA.

At Lane Powell, every client relationship begins with our Cyber Health Assessment, a free comprehensive analysis of the key facets of the privacy and data security environment resulting in a tailored suite of integrated privacy law compliance and risk mitigation services and pricing options.

From preliminary risk assessment of privacy and data security policies to breach preparedness and response, our Privacy & Data Security Team crafts custom strategies to assist clients in effectively and efficiently minimizing legal and reputational risk related to the collection, use, storage and loss of sensitive data.

Proactive Data Security Counseling

- Evaluate and assess cyber liability risk.
- Advise regarding compliance with state, federal and international privacy and data security regulations, including GDPR and CCPA.
- Structure procedures to best facilitate HIPAA compliance and audits.
- Perform security assessments, craft data breach response plans, and develop and facilitate data breach table top exercises.
- Train employees to minimize the risk of intentional theft or negligent loss of data.
- Evaluate and negotiate cyber liability insurance options.
- Advise officers and directors on disclosure obligations regarding cybersecurity and privacy matters.

Compliance Advice and Implementation

- Design privacy law compliance strategies to fit your business plan.
- Create effective privacy notices/policies, terms of use and end user licensing agreements for web, IoT, AI and mobile application implementation.
- Prepare startups for market via website readiness and internal privacy policy development.
• Prepare legitimate interest assessments and risk assessments, as necessary to achieve GDPR and/or CCPA compliance.
• Develop internal policies to control and manage sensitive data, select data processing vendors, and respond to consumer requests to exercise their rights under the GDPR and/or CCPA.
• Provide corporate training from C-Suite to staff on internal protocols and best practices for privacy law compliance and security risk mitigation.

Data Privacy Considerations in Corporate Transactions

• Data protection addenda (DPA) due diligence and drafting.
• Draft and negotiate commercial contracts including SaaS agreements, cloud-based service contracts, DevOps and subscription services agreements, and other technology product and service offerings.
• Analysis and risk assessment of existing third party contracts with technology and marketing vendors.
• Merger and acquisition due diligence regarding data as a transferable asset, consumer and employee data privacy considerations, and use and transfer of technology.

Data Breach Strategy Development and Response

• Assist in the implementation of a data breach response plan.
• Coordinate breach assessments and action plans.
• Coordinate with local and national law enforcement personnel when necessary.
• Ensure compliance with state, national and international breach notification laws.
• Represent clients in regulatory investigations and civil lawsuits that arise from data breach events.

Experience

Ransomware Attack
Represented skilled nursing facility with respect to a ransomware incident, including investigation of incident, HIPAA breach analysis and notice issues, and appropriate mitigation and response issues.

HIPAA-Related Agreements
Represented national employer in preparation of agreement with medical university for use where medical student interns receiving certain training experiences on client employer’s premises, to make sure that HIPAA-based privacy duties are met.

HIPAA Issues Implicated by Witness Subpoena
Represented national senior living and long term care provider with respect to HIPAA and other privacy concerns implicated when its medical staff was subpoenaed to testify as a third-party witness in a lawsuit. Negotiated with counsel in the preparation and entry of an appropriate Protective Order, including appropriate procedures to comply with HIPAA and otherwise comply with privacy rights and duties.

Social Media Policy Development and Implementation
Prepared training materials for use by professional trade group organization with respect to development,
implementation and enforcement of appropriate social media policies for HIPAA-covered entities' and other care providers.

**HIPAA Compliance / Online Health Application**

Prepared HIPAA and other privacy related policies for developer of online-accessed health-related application.