Data Privacy & Cybersecurity Compliance

Businesses and organizations of all sizes collect, store, and share personal information about individuals with whom they interact, and that data ranks among a company's most important assets.

While new technologies and easy access to information allows for greater innovation and enhanced delivery of products and services, that is accompanied by an ever-increasing potential for liability, and the protection of data maintained on consumers and employees requires a broad range of legal compliance activities. It is important to prioritize and protect sensitive, confidential and proprietary information. If a breach or data loss occurs, it immediately places a company's reputation and bottom line at risk.

Lathrop GPM's Data Privacy & Cybersecurity Compliance group has a tradition of excellence in this evolving area of the law, and routinely guides clients through the high-paced investigation, notification and response involved in a data breach or loss. Our team brings special experience in laws and regulations relating to information technology, employment, health care, insurance, and financial institutions, as well as certifications in both United States and European data privacy law (CIPP/US and CIPP/E) from the International Association of Privacy Professionals that allow the team to provide exceptional legal services.

With an eye toward prevention, our multidisciplinary team of attorneys and data specialists can assess regulatory requirements, identify risk and develop strategies to protect personally identifiable information (PII), personal health information (PHI) and proprietary data. In addition, our insurance lawyers in the practice group can assist in considering appropriate cyberinsurance coverage.

Our data privacy and security experience extends to public and private organizations across industries such as healthcare, insurance, finance, technology, media, and education. We engage in a wide variety of data

litigation and regulatory matters, from class actions under the Telephone Consumer Protection Act to individual claims. We deal with the more than 50 laws enforced by the Federal Trade Commission and state attorneys general, as well as the EU and other international data protection authorities.

Our attorneys are nationally recognized speakers and authors on topics such as HIPAA, HITECH, cybersecurity, data breach, cyber insurance coverage, and social media. We assist with the drafting of privacy policies, terms of use for websites and mobile applications, service level agreements and other key documents. We help our clients navigate the patchwork of state, federal and international regulation that has emerged to govern data privacy and security, including compliance with the European data privacy law known as the GDPR, and the California Consumer Privacy Act (CCPA).

We regularly advise clients in the following areas:

Data Breach Response and Cybersecurity Readiness

Data breaches, biosensors, "big data," the "internet of things," credit card fraud, stolen data, and data monetization efforts are all pushing the limits of privacy advocates, regulators, consumers, and lawyers who advise businesses on the use of information technology, data privacy, and security issues. It is not a question of whether unauthorized access, an incident, or a data breach will occur, but when. Lathrop GPM helps clients become ready for any unauthorized incident or data breach and offers proactive best practices to mitigate risk. The team's experience includes:

- Incident and breach risk assessment
- Management of data breach response
- Individual and regulatory notifications
- Regulatory investigation response
  - Office for Civil Rights
  - Federal Trade Commission
  - State Attorneys General

- State Insurance Commissioners
- Media notification
- Insurance tender and response

Data Protection and Privacy Policies & Procedures

The Lathrop GPM team works closely with clients to establish and implement data breach response plans that enable them to comply promptly with legal requirements and reduce the risk of serious reputational and financial harm. The team's experience includes:

- Assessment of obligations
  - HIPAA/HITECH
  - Gramm-Leach-Bliley
  - Insurance regulations
  - FDIC and banking regulations
  - State privacy/security laws
  - PCI DSS compliance
- Key Data Policies & Documents
  - HIPAA/HITECH policies
  - Business associate agreements
  - Corporate privacy policies and procedures
  - Information management and life-cycle policies
  - Website privacy policies and terms of use
  - Information technology usage policies
  - Information governance policies
  - Document retention and destruction policies
  - Policies to safeguard confidential and proprietary information
  - Best practices for use of behavioral advertising, search engine optimization (SEO), geolocation, "cookies," and other tracking technologies
  - Advising regarding SMS text messaging campaigns
  - Advising regarding vendor management programs, including information security policies and procedures, vendor information security, and privacy contracts and addendums
  - Confidentiality agreements

- Training and education

Cybersecurity Insurance

Lathrop GPM attorneys have significant experience navigating the unique and complex issues related to the cybersecurity insurance market. The team helps clients mitigate losses from cyber incidents through:

- Evaluation of various types of cybersecurity coverages and coordination with other traditional coverages
- Preparation of contract provisions with appropriate insurance obligations to address privacy and data security exposures
- Representation of clients in pursuing claims for coverage

Social Media, Privacy, and Technology in the Workplace

Well-crafted social media, privacy, and technology policies that balance company needs and concerns against employees' legal rights are important tools for any business. Lathrop GPM's team is experienced in managing these competing legal risks. Our attorneys advise clients regarding:

- Compliance with FRCA
- Monitoring of employee communications
- Video surveillance
- Pre-employment background checks
- Post hire investigations
- Investigations of employee misconduct and theft
- "Bring your own device" (BYOD) policies
- Use of social media as a business tool
- Social media usage policies

Litigation

- Individual data and privacy litigation
- Class-action litigation defense
- TCPA litigation defense

Global Privacy Compliance

Every second, personal data is collected, used, processed, or moved across borders. As an increasing number of foreign laws attempt to protect personal data, differing country-specific requirements create a maze of global privacy considerations for any business operating across borders. Our team advises clients regarding compliance with international data protection laws, including the EU Data Directive and the General Data Protection Regulation (GDPR) (including model contracts, binding corporate rules, Privacy Shield, and other EU data transfer mechanisms), as well as the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and Canada's stringent new anti-spam law.

Representative Experience

- We have managed a wide variety of data loss and data breach incidents such as:
  - Thefts of laptops, mobile phones and other devices containing PII and/or PHI
  - Infiltrations of company databases for corporate or government espionage
  - Thefts of credit card information and subsequent improper charges
  - Postings of key trade secret information on social media and other websites
  - Employee transfers of proprietary data to personal email, external drives, cloud, etc.
  - Dedicated Denial of Service attacks upon company websites
- Representation of a hospital in the coordination of data breach investigation and response following a vendor's inadvertent internet publication of financial information of over 8,000 individuals. The subsequent investigation by Office for Civil Rights was resolved without fines or penalties through demonstration of voluntary compliance including timely notification, mitigation of harm to individuals, and revision of policies and procedures.
- Resolution of multiple Office for Civil Rights investigations of healthcare providers related to HIPAA complaints related to patient access, accounting of disclosures, access to electronic systems, inadvertent disclosures, and loss of paper records.

- Investigation and coordination of a healthcare facility's response of a complaint involving improper access to patient data by an employee. Our representation included investigation and termination of the employee, development and coordination of breach notification in compliance with HIPAA and state requirements, and mandatory reporting to the Office of Civil Rights and state licensure board.
- Counseling numerous health care providers, health plans, and business associates in the development and implementation of more robust HIPAA Compliance programs to integrate requirements of the Omnibus HIPAA regulations promulgated in January 2013.

Resources

Below are published resources, typically updated annually:

- *A Legal Guide to Privacy and Data Security (2024)*
- *A Legal Guide to Technology Transactions*
- *A Legal Guide to the Use of Social Media in the Workplace*